

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-111679

(43)Date of publication of application : 30.04.1996

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

G06F 17/60

G09C 1/00

(21)Application number : 06-245571

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 11.10.1994

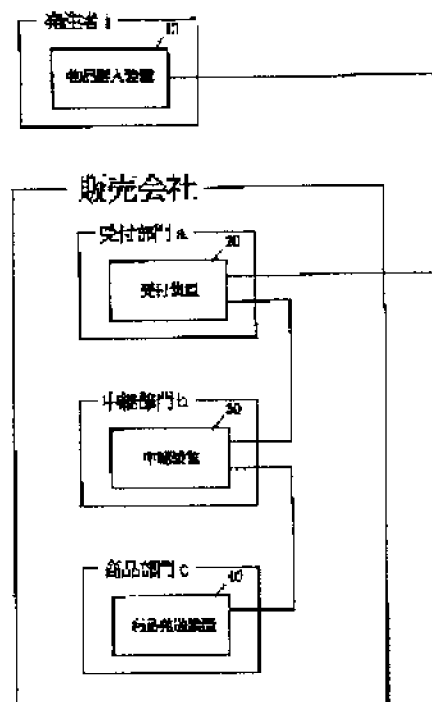
(72)Inventor : OMORI MOTOJI
TATEBAYASHI MAKOTO

(54) MAIL ORDER SYSTEM

(57)Abstract:

PURPOSE: To surely protect the privacy of an ordering person concerning the mail order system for ordering and purchasing merchandise through a communication network.

CONSTITUTION: An ordering person (i) doubly ciphers the merchandise code of order merchandise by using two cryptographic keys and those two cryptographic keys are respectively ciphered for a relay section (b) and a merchandise section (c). Then, the doubly ciphered merchandise code is transmitted to a reception section (a) together with the two ciphered cryptographic keys and the identifier of the ordering person. The reception section (a) transmits the received ciphered order contents to the relay section (b) together with a reference number Ref 1. Among the received ciphered order contents, the cryptographic key ciphered for the relay section is deciphered and the doubly ciphered merchandise code is partially deciphered by the relay section (b). Then, the partially deciphered merchandise code is transmitted to the merchandise section (c) together with the cryptographic key ciphered for the merchandise section and a reference number Ref 2. The merchandise section (c) decipheres the cryptographic key ciphered for the merchandise section, further decipheres the partially deciphered merchandise code and recognizes the name of ordered merchandise.



LEGAL STATUS

[Date of request for examination] 10.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3496774

[Date of registration] 28.11.2003

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-111679

(43) 公開日 平成 8 年 (1996) 4 月 30 日

(51) Int. Cl. ⁷

識別記号

F I

H04L 9/00

9/10

9/12

H04L 9/00

2

G06F 15/21

330

審査請求 未請求 請求項の数 9 O L (全33頁) 最終頁に続く

(21) 出願番号 特願平6-245571

(22) 出願日 平成 6 年 (1994) 10 月 11 日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

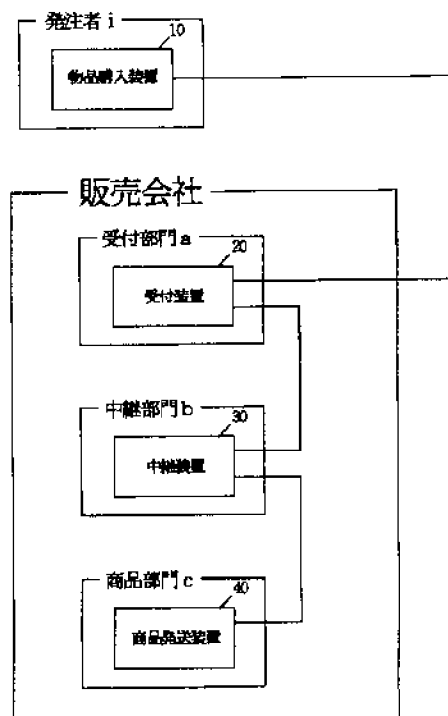
(74) 代理人 弁理士 小笠原 史朗

(54) 【発明の名称】 通信販売システム

(57) 【要約】 (修正有)

【目的】 通信ネットワークを介して商品を注文購入する通信販売システムにおいて、発注者のプライバシーを確実に保護する。

【構成】 発注者 i は、発注商品の商品コードを、2つの暗号鍵を用いて二重に暗号化し、その2つの暗号鍵をそれぞれ、中継部門 b、商品部門 c 向けに暗号化する。そして、二重に暗号化した商品コードを、暗号化した2つの暗号鍵および発注者の識別子と共に受付部門 a に送る。受付部門 a は、受信した暗号化発注内容を、照会番号 Ref 1 と共に中継部門 b に送る。中継部門 b は、受信した暗号化発注内容のうち、中継部門向けに暗号化された暗号鍵を復号し、二重に暗号化されている商品コードを一部復号する。そして、一部復号された商品コードを、商品部門向けに暗号化された暗号鍵および照会番号 Ref 2 と共に商品部門 c へ送る。商品部門 c は、商品部門向けに暗号化された暗号鍵を復号して、一部復号された商品コードをさらに復号し、発注された商品名を知る。



【特許請求の範囲】

【請求項 1】 複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、

前記発注者、前記受付部門および前記商品部門には、それぞれ、物品購入装置、受付装置および商品発送装置が設けられており、

前記物品購入装置は、

電子データから成る鍵を発生する鍵発生手段と、

前記鍵を用いて、商品の発注内容を暗号化する発注内容暗号化手段と、

前記鍵を暗号化する鍵暗号化手段と、

前記暗号化された商品の発注内容に、前記暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第 1 の送信手段とを含み、

前記受付装置は、
前記物品購入装置から送信されてくるデータを受信する第 1 の受信手段と、

前記第 1 の受信手段が受信した前記本人確認情報が、正当なものか否かを確認する確認手段と、

前記確認手段によって前記本人確認情報が正当なものと確認された場合、前記第 1 の受信手段が受信した前記暗号化された商品の発注内容と前記暗号化された鍵とに、

前記発注者の識別情報とは異なる仮名情報を付加して、前記商品発送装置に送信する第 2 の送信手段と、

前記発注者の識別情報と前記仮名情報との対応関係を記憶する対応関係記憶手段とを含み、

前記商品発送装置は、
前記受付装置から送信されてくるデータを受信する第 2 の受信手段と、

前記第 2 の受信手段が受信した前記暗号化された鍵を復号する鍵復号手段と、

前記復号された鍵を用いて、前記第 2 の受信手段が受信した前記暗号化された商品の発注内容を復号する発注内容復号手段と、

前記電子的商品を保管する商品保管手段と、
前記復号された商品の発注内容に基づいて、前記商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、

前記読み出し手段により読み出された電子的商品を、前記復号された鍵を用いて暗号化する商品暗号化手段と、

前記暗号化された電子的商品を、前記第 2 の受信手段が受信した前記仮名情報と共に、前記受付装置に送信する第 3 の送信手段とを含み、

前記受付装置は、さらに前記商品発送装置から送信されてくるデータを受信する第 3 の受信手段と、

前記第 3 の受信手段が受信した前記仮名情報に基づいて、前記対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、

前記第 3 の受信手段が受信した前記暗号化された電子的

商品を、前記発注者特定手段により特定された発注者の前記物品購入装置に送信する第 4 の送信手段とを含み、
前記物品購入装置は、前記受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含む、通信販売システム。

【請求項 2】 前記仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項 1 に記載の通信販売システム。

【請求項 3】 複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、

前記発注者、前記受付部門、前記中継部門および前記商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、

前記物品購入装置は、

電子データから成る第 1 および第 2 の鍵を発生する鍵発生手段と、

前記第 1 および第 2 の鍵を用いて、商品の発注内容を 2 重に暗号化する発注内容暗号化手段と、

前記第 1 および第 2 の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、

前記 2 重に暗号化された商品の発注内容に、前記暗号化された第 1 および第 2 の鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第 1 の送信手段とを含み、

前記受付装置は、

前記物品購入装置から送信されてくるデータを受信する第 1 の受信手段と、

前記第 1 の受信手段が受信した前記本人確認情報が、正当なものか否かを確認する確認手段と、

前記確認手段によって前記本人確認情報が正当なものと確認された場合、前記第 1 の受信手段が受信した前記 2 重に暗号化された商品の発注内容と前記暗号化された第 1 および第 2 の鍵とに、前記発注者の識別情報とは異なる第 1 の仮名情報を付加して、前記中継装置に送信する第 2 の送信手段と、

前記発注者の識別情報と前記第 1 の仮名情報との対応関係を記憶する第 1 の対応関係記憶手段とを含み、

前記中継装置は、

前記受付装置から送信されてくるデータを受信する第 2 の受信手段と、

前記第 2 の受信手段が受信した前記暗号化された第 1 の鍵を復号する第 1 の鍵復号手段と、

前記復号された第 1 の鍵を用いて、前記第 2 の受信手段が受信した前記 2 重に暗号化された商品の発注内容を、部分的に復号する第 1 の発注内容復号手段と、

前記部分的に復号された商品の発注内容に、前記第 1 の仮名情報とは異なる第 2 の仮名情報を付加して、前記商品発送装置に送信する第 3 の送信手段と、

前記第 1 の仮名情報と前記第 2 の仮名情報との対応関係

を記憶する第 2 の対応関係記憶手段とを含み、
 前記商品発送装置は、
 前記中継装置から送信されてくるデータを受信する第 3 の受信手段と、
 前記第 3 の受信手段が受信した前記暗号化された第 2 の鍵を復号する第 2 の鍵復号手段と、
 前記復号された第 2 の鍵を用いて、前記第 3 の受信手段が受信した前記部分的に復号された商品の発注内容を全面的に復号する第 2 の発注内容復号手段と、
 前記電子的商品を保管する商品保管手段と、
 前記全面的に復号された商品の発注内容に基づいて、前記商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、
 前記読み出し手段により読み出された電子的商品を、前記復号された第 2 の鍵を用いて暗号化する第 1 の商品暗号化手段と、
 前記第 2 の鍵を用いて暗号化された電子的商品を、前記第 3 の受信手段が受信した前記第 2 の仮名情報と共に、前記中継装置に送信する第 4 の送信手段とを含み、
 前記中継装置は、さらに前記商品発送装置から送信されてくるデータを受信する第 4 の受信手段と、
 前記第 4 の受信手段が受信した前記暗号化された電子的商品を、対応する前記第 1 の鍵を用いて 2 重に暗号化する第 2 の商品暗号化手段と、
 前記第 4 の受信手段が受信した前記第 2 の仮名情報に基づいて、前記第 2 の対応関係記憶手段を検索し、当該第 2 の仮名情報に対応する前記第 1 の仮名情報を特定する仮名情報特定手段と、
 前記第 2 の鍵を用いて 2 重に暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第 1 の仮名情報と共に、前記受付装置に送信する第 5 の送信手段とを含み、
 前記受付装置は、さらに前記中継装置から送信されてくるデータを受信する第 5 の受信手段と、
 前記第 5 の受信手段が受信した前記第 1 の仮名情報に基づいて、前記第 1 の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、
 前記第 5 の受信手段が受信した前記 2 重に暗号化された電子的商品を、前記発注者特定手段により特定された発注者の前記物品購入装置に送信する第 6 の送信手段とを含み、
 前記物品購入装置は、前記受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含む、通信販売システム。

【請求項 4】 前記第 1 および第 2 の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項 3 に記載の通信販売システム。

【請求項 5】 複数の発注者、受付部門、 n 個 (n は 2 以上の整数) の中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売

システムであって、
 前記発注者、前記受付部門、前記中継部門および前記商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、
 前記物品購入装置は、
 電子データから成る第 1 および第 2 の鍵を発生する鍵発生手段と、
 前記第 1 および第 2 の鍵を用いて、商品の発注内容を 2 重に暗号化する発注内容暗号化手段と、
 前記第 1 および第 2 の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、
 前記 2 重に暗号化された商品の発注内容に、前記暗号化された第 1 および第 2 の鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第 1 の送信手段とを含み、
 前記受付装置は、
 前記物品購入装置から送信されてくるデータを受信する第 1 の受信手段と、
 前記第 1 の受信手段が受信した前記本人確認情報が、正当なものか否かを確認する確認手段と、
 前記確認手段によって前記本人確認情報が正当なものと確認された場合、前記第 1 の受信手段が受信した前記 2 重に暗号化された商品の発注内容と、前記暗号化された第 1 および第 2 の鍵と共に、前記発注者の識別情報とは異なる第 1 の仮名情報を付加して、第 1 番目の前記中継部門に属する中継装置に送信する第 2 の送信手段と、
 前記発注者の識別情報と前記第 1 の仮名情報との対応関係を記憶する第 1 の対応関係記憶手段とを含み、
 第 1 番目の前記中継部門に属する中継装置は、
 前記受付装置から送信されてくるデータを受信する第 2 の受信手段と、
 前記第 2 の受信手段が受信した前記暗号化された第 1 の鍵を復号する第 1 の鍵復号手段と、
 前記復号された第 1 の鍵を用いて、前記第 2 の受信手段が受信した前記 2 重に暗号化された商品の発注内容を、部分的に復号する第 1 の発注内容復号手段と、
 前記部分的に復号された商品の発注内容に、前記第 1 の仮名情報とは異なる第 2 の仮名情報を付加して、第 2 番目の前記中継装置に属する中継装置に送信する第 3 の送信手段と、
 前記第 1 の仮名情報と前記第 2 の仮名情報との対応関係を記憶する第 2 の対応関係記憶手段とを含み、
 第 m 番目 (m は、 $2 \leq m \leq n-1$ の整数) の前記中継部門に属する中継装置は、
 第 $(m-1)$ 番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第 3 の受信手段と、
 前記第 3 の受信手段が受信した前記部分的に復号された商品の発注内容に、第 m の仮名情報とは異なる第 $(m-1)$ の仮名情報を付加して、第 $(m+1)$ 番目の中継部門に属する中継装置に送信する第 4 の送信手段と、

前記第 m の仮名情報と前記第 $(m-1)$ の仮名情報との対応関係を記憶する第3の対応関係記憶手段とを含み、第 n 番目の前記中継部門に属する中継装置は、第 $(n-1)$ 番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第4の受信手段と、前記第4の受信手段が受信した前記部分的に復号された商品の発注内容に、第 n の仮名情報とは異なる第 $(n+1)$ の仮名情報を付加して、前記商品発送装置に送信する第5の送信手段と、

前記第 n の仮名情報と前記第 $(n+1)$ の仮名情報との対応関係を記憶する第4の対応関係記憶手段とを含み、前記商品発送装置は、第 n 番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第5の受信手段と、

前記第5の受信手段が受信した前記暗号化された第2の鍵を復号する第2の鍵復号手段と、

前記復号された第2の鍵を用いて、前記第5の受信手段が受信した前記部分的に復号された商品の発注内容を全面的に復号する第2の発注内容復号手段と、前記電子的商品を保管する商品保管手段と、

前記全面的に復号された商品の発注内容に基づいて、前記商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、

前記読み出し手段により読み出された電子的商品を、前記復号された第2の鍵を用いて暗号化する第1の商品暗号化手段と、

前記第2の鍵を用いて暗号化された電子的商品を、前記第5の受信手段が受信した前記第 $(n+1)$ の仮名情報と共に、第 n 番目の前記中継部門に属する中継装置に送信する第6の送信手段とを含み、

第 n 番目の前記中継部門に属する中継装置は、さらに前記商品発送装置から送信されてくるデータを受信する第6の受信手段と、

前記第6の受信手段が受信した前記第 $(n+1)$ の仮名情報に基づいて、前記第4の対応関係記憶手段を検索し、当該第 $(n-1)$ の仮名情報に対応する第 n の仮名情報を特定する第1の仮名情報特定手段と、

前記第6の受信手段が受信した前記暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第 n の仮名情報と共に、第 m 番目の前記中継部門に属する中継装置に送信する第7の送信手段とを含み、

第 m 番目の前記中継部門に属する中継装置は、さらに第 $(m-1)$ 番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第7の受信手段と、

前記第7の受信手段が受信した前記第 m の仮名情報に基づいて、前記第3の対応関係記憶手段を検索し、当該第 m の仮名情報に対応する第 $(m-1)$ の仮名情報を特定する第2の仮名情報特定手段と、

前記第7の受信手段が受信した前記暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第

$(m-1)$ の仮名情報と共に、第 $(m-1)$ 番目の前記中継部門に属する中継装置に送信する第8の送信手段とを含み、

第1番目の前記中継部門に属する中継装置は、さらに第2番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第8の受信手段と、

前記第8の受信手段が受信した前記暗号化された電子的商品を、対応する前記第1の暗号鍵を用いて2重に暗号化する第2の商品暗号化手段と、

前記第8の受信手段が受信した前記第2の仮名情報に基づいて、前記第3の対応関係記憶手段を検索し、当該第2の仮名情報に対応する第1の仮名情報を特定する第3の仮名情報特定手段と、

前記第8の受信手段が受信した前記暗号化された電子的商品を、前記仮名情報特定手段により特定された前記第1の仮名情報と共に、前記受付装置に送信する第9の送信手段とを含み、

前記受付装置は、さらに第1番目の前記中継部門に属する中継装置から送信されてくるデータを受信する第9の受信手段と、

前記第9の受信手段が受信した前記第1の仮名情報に基づいて、前記第1の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、

前記第9の受信手段が受信した前記2重に暗号化された電子的商品を、前記発注者特定手段により特定された発注者の前記物品購入装置に送信する第6の送信手段とを含み、

前記物品購入装置は、前記受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含む、通信販売システム。

【請求項6】 複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、

前記発注者においては、

電子データから成る鍵を発生する鍵発生ステップと、

前記鍵を用いて、商品の発注内容を暗号化する発注内容暗号化ステップと、

前記鍵を暗号化する鍵暗号化ステップと、

前記暗号化された商品の発注内容に、前記暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第1の送信ステップとを実行し、

前記受付部門においては、

前記発注者から送信されてくるデータを受信する第1の受信ステップと、

前記第1の受信ステップで受信した前記本人確認情報が、正当なものか否かを確認する確認ステップと、

前記確認ステップによって前記本人確認情報が正当なものと確認された場合、前記第1の受信ステップで受信した前記暗号化された商品の発注内容と前記暗号化された

鍵とに、前記発注者の識別情報とは異なる仮名情報を付加して、前記商品発送装置に送信する第 2 の送信ステップと、
 前記発注者の識別情報と前記仮名情報との対応関係を記憶する対応関係記憶ステップとを実行し、
 前記商品部門においては、
 前記受付部門から送信されてくるデータを受信する第 2 の受信ステップと、
 前記第 2 の受信ステップで受信した前記暗号化された鍵を復号する鍵復号ステップと、
 前記復号された鍵を用いて、前記第 2 の受信ステップで受信した前記暗号化された商品の発注内容を復号する発注内容復号ステップと、
 前記復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が前記受付部門にわからないように梱包封印する梱包封印ステップと、
 前記梱包封印された商品を、前記第 2 の受信ステップで受信した前記仮名情報と共に、前記受付部門に発送する第 1 の発送ステップとを実行し、
 前記受付部門においては、さらに前記商品部門から受け取った前記仮名情報に基づいて、前記対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、
 前記商品部門から受け取った前記梱包封印された商品を、前記発注者特定ステップで特定された発注者に発送する第 2 の発送ステップとを実行することを特徴とする、通信販売方法。

【請求項 7】 前記仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項 6 に記載の通信販売方法。

【請求項 8】 複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、
 前記発注者においては、
 電子データから成る第 1 および第 2 の鍵を発生する鍵発生ステップと、
 前記第 1 および第 2 の鍵を用いて、商品の発注内容を 2 重に暗号化する発注内容暗号化ステップと、
 前記第 1 および第 2 の鍵を、それぞれ別個に暗号化する鍵暗号化ステップと、
 前記 2 重に暗号化された商品の発注内容に、前記暗号化された第 1 および第 2 の鍵と、発注者の識別情報と、本人確認情報とを付加して、前記受付装置に送信する第 1 の送信ステップとを含み、
 前記受付部門においては、
 前記物品購入装置から送信されてくるデータを受信する第 1 の受信ステップと、
 前記第 1 の受信ステップで受信した前記本人確認情報が、正当なものか否かを確認する確認ステップと、
 前記確認ステップによって前記本人確認情報が正当なも

のと確認された場合、前記第 1 の受信ステップで受信した前記 2 重に暗号化された商品の発注内容と前記暗号化された第 1 および第 2 の鍵とに、前記発注者の識別情報とは異なる第 1 の仮名情報を付加して、前記中継装置に送信する第 2 の送信ステップと、
 前記発注者の識別情報と前記第 1 の仮名情報との対応関係を記憶する第 1 の対応関係記憶ステップとを実行し、
 前記中継部門においては、
 前記受付装置から送信されてくるデータを受信する第 2 の受信ステップと、
 前記第 2 の受信ステップで受信した前記暗号化された第 1 の鍵を復号する第 1 の鍵復号ステップと、
 前記復号された第 1 の鍵を用いて、前記第 2 の受信ステップで受信した前記 2 重に暗号化された商品の発注内容を、部分的に復号する第 1 の発注内容復号ステップと、
 前記部分的に復号された商品の発注内容に、前記第 1 の仮名情報とは異なる第 2 の仮名情報を付加して、前記商品発送装置に送信する第 3 の送信ステップと、
 前記第 1 の仮名情報と前記第 2 の仮名情報との対応関係を記憶する第 2 の対応関係記憶ステップとを実行し、
 前記商品部門においては、
 前記中継装置から送信されてくるデータを受信する第 3 の受信ステップと、
 前記第 3 の受信ステップで受信した前記暗号化された第 2 の鍵を復号する第 2 の鍵復号ステップと、
 前記復号された第 2 の鍵を用いて、前記第 3 の受信ステップで受信した前記部分的に復号された商品の発注内容を全面的に復号する第 2 の発注内容復号ステップと、
 前記全面的に復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が前記受付部門にわからないように梱包封印する第 1 の梱包封印ステップと、
 前記梱包封印された商品を、前記第 2 の受信ステップで受信した前記仮名情報と共に、前記中継部門に発送する第 1 の発送ステップとを実行し、
 前記中継部門においては、さらに前記商品部門から受け取った前記梱包封印された商品を、さらに 2 重に梱包封印する第 2 の梱包封印ステップと、
 前記商品部門から受け取った前記第 2 の仮名情報に基づいて、前記第 2 の対応関係記憶ステップで記憶した対応関係を検索し、当該第 2 の仮名情報に対応する前記第 1 の仮名情報を特定する仮名情報特定ステップと、
 前記 2 重に梱包封印された商品を、前記仮名情報特定ステップにより特定された前記第 1 の仮名情報と共に、前記受付部門に発送する第 2 の発送ステップとを実行し、
 前記受付部門においては、さらに前記中継部門から受け取った前記第 1 の仮名情報に基づいて、前記第 1 の対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、
 前記中継部門から受け取った前記 2 重に梱包封印された

商品を、前記発注者特定ステップにより特定された発注者に発送する第3の発送ステップとを実行することを特徴とする、通信販売方法。

【請求項9】 前記第1および第2の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする、請求項8に記載の通信販売方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、通信販売システムに関し、より特定的には、通信ネットワークを用いて、商品の発注と流通を行うシステムに関する。

【0002】

【従来の技術】近年、市場ではカタログを用いた通信販売による物品の売買が盛んになってきており、徐々に販売高を伸ばしている。また、パーソナルコンピュータ（以下、パソコンと略称する）通信などのネットワーク網が普及してきており、電話における口頭での受け渡しではどうしても間違いが出るような大量かつ詳細な情報も、パソコン通信では正確に伝えられることもあって、パソコン通信を用いた通信ネットワークを用いた通信販売が、大いに発展しつつある。特に、コンピュータの業務用ソフトウェアやゲーム用ソフトウェア、そしてマルチメディア電子百科辞典などの電子的商品が、頻繁に取り引きされている。さらに、パソコン通信、デジタルCATV網、B-ISDN網などの通信ネットワークを用いた通信販売網で、電子的商品の販売や情報サービスの提供が多く行われつつある。この場合、もちろん無形商品である電子的商品は、発注を受けたネットワーク網を介して発注者の元に送られる。

【0003】図15は、従来の通信ネットワークを用いた通信販売システムの構成を示す図である。図15において、初めに、各発注者5は、販売会社6に、名前とパソコン通信アドレスと振替指定銀行口座などを記した通信販売システム申込書を送り、銀行には、販売会社から正当な請求があった場合には、その口座から口座所有者の許可なしに振り替えても構わないという内容の契約書を送っておく。この手続きにより、発注者5は、本システムにおける発注者識別子UIDを得る。

【0004】図15において、発注者5と販売会社6は、パソコン通信でつながっている。発注者5は、電子的商品を販売会社6に発注し、販売会社6から送られてくる電子的商品を受け取る物品購入装置50を所持している。当該物品購入装置50は、例えばパソコンのソフトウェアとして実現される。また、電子的商品としては、パソコン上で利用できるコンピュータソフトウェアやマルチメディアソフトウェアなどが考えられる。また販売会社6には、発注者から送られてくる発注情報を受け取る受付装置60と、電子的商品を保管しておく商品保管部61と、各発注者の識別子、パソコン通信アドレスおよび振替指定銀行口座等を保管しておく個人データ

格納部62と、価格などの商品データを格納している商品データ格納部63とが設けられている。

【0005】発注者は、物品購入装置50に欲しい電子的商品の商品コードPIDを入力する。応じて、物品購入装置50は、発注者の識別子UIDと商品コードPIDを、パソコン通信を介して販売会社6に送信する。

【0006】販売会社6では、受付装置60が、発注者から送られてきた識別子UIDと商品コードPIDとを受信する。次に、受付装置60は、商品コードPIDに対応する電子的商品PDTを商品保管部60から取り出すと共に、商品データ格納部63を検索して電子的商品PIDに対応する価格Prを求める。次に、受付装置60は、送られてきた識別子UIDをもとに、個人データ格納部62から、対応する発注者のパソコン通信アドレスと、振替指定銀行口座とを読み出す。次に、受付装置60は、価格Prを発注者の振替指定銀行口座から販売会社の口座へ振り替えしてもらうように、銀行に依頼する。次に、受付装置60は、パソコン通信アドレスを参照して、発注者に発注を受けた商品PDTを送信する。

【0007】発注者においては、物品発注装置50が、発注した電子的商品PDTを受け取り、当該受け取った電子的商品PDTをパソコンなどのハードディスクに保存して使用する。

【0008】なお、販売する商品が電子的商品でない場合にも、パソコン通信を用いて商品の発注を行い、販売会社は発注者の住所へ物理的な手段で発送することにより、商品の売買を行うことができる。

【0009】

【発明が解決しようとする課題】しかしながら、上記従来の通信販売システムでは、通信ネットワークを用いて商品の転送を行う必要性がある以上、通信の相手先を特定する必要がある。また、銀行振替やクレジットカードシステムなどの代金回収方法を用いようすると、当然発注者を特定しなくてはならない。従って、販売会社に「誰が何を買ったか」という情報が伝わってしまうという特性がある。旧来の店頭での現金による物品販売では、発注者である購入者が名前を提示する必要がなく、販売店が「誰が買っているのか」は完全にはわからなかったことに比較し、上述の特性は通信ネットワークを用いた通信販売を実現するにあたって大きな問題点である。現在、各個人のプライバシーの保護が大きく叫ばれており、この問題点は、通信ネットワークを用いた通信販売システムの普及に影響を及ぼすものと思われる。

【0010】それゆえに、本発明の目的は、発注者が通信ネットワークを介して商品を注文購入する際に、発注者のプライバシー（例えば、「誰が何を買ったか」という情報）を確実に保護でき、しかもクレジットカードや銀行引き落としなどの既存の決済システムをそのまま使用できる通信販売システムを提供することである。

【0011】

【課題を解決するための手段】請求項 1 に係る発明は、複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、発注者、受付部門および商品部門には、それぞれ、物品購入装置、受付装置および商品発送装置が設けられており、物品購入装置は、電子データから成る鍵を発生する鍵発生手段と、鍵を用いて、商品の発注内容を暗号化する発注内容暗号化手段と、鍵を暗号化する鍵暗号化手段と、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第 1 の送信手段とを含み、受付装置は、物品購入装置から送信されてくるデータを受信する第 1 の受信手段と、第 1 の受信手段が受信した本人確認情報が、正当なものか否かを確認する確認手段と、確認手段によって本人確認情報が正当なものと確認された場合、第 1 の受信手段が受信した暗号化された商品の発注内容と暗号化された鍵とに、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する第 2 の送信手段と、発注者の識別情報と仮名情報との対応関係を記憶する対応関係記憶手段とを含み、商品発送装置は、受付装置から送信されてくるデータを受信する第 2 の受信手段と、第 2 の受信手段が受信した暗号化された鍵を復号する鍵復号手段と、復号された鍵を用いて、第 2 の受信手段が受信した暗号化された商品の発注内容を復号する発注内容復号手段と、電子的商品を保管する商品保管手段と、復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、読み出し手段により読み出された電子的商品を、復号された鍵を用いて暗号化する商品暗号化手段と、暗号化された電子的商品を、第 2 の受信手段が受信した仮名情報と共に、受付装置に送信する第 3 の送信手段とを含み、受付装置は、さらに商品発送装置から送信されてくるデータを受信する第 3 の受信手段と、第 3 の受信手段が受信した仮名情報に基づいて、対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、第 3 の受信手段が受信した暗号化された電子的商品を、発注者特定手段により特定された発注者の物品購入装置に送信する第 4 の送信手段とを含み、物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含んでいる。

【0012】請求項 2 に係る発明は、請求項 1 の発明において、仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【0013】請求項 3 に係る発明は、複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、発注者、受付部門、中継部門および商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、物品購入装置

は、電子データから成る第 1 および第 2 の鍵を発生する鍵発生手段と、第 1 および第 2 の鍵を用いて、商品の発注内容を 2 重に暗号化する発注内容暗号化手段と、第 1 および第 2 の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、2 重に暗号化された商品の発注内容に、暗号化された第 1 および第 2 の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第 1 の送信手段とを含み、受付装置は、物品購入装置から送信されてくるデータを受信する第 1 の受信手段と、第 1 の受信手段が受信した本人確認情報が、正当なものか否かを確認する確認手段と、確認手段によって本人確認情報が正当なものと確認された場合、第 1 の受信手段が受信した 2 重に暗号化された商品の発注内容と暗号化された第 1 および第 2 の鍵とに、発注者の識別情報とは異なる第 1 の仮名情報を付加して、中継装置に送信する第 2 の送信手段と、発注者の識別情報と第 1 の仮名情報との対応関係を記憶する第 1 の対応関係記憶手段とを含み、中継装置は、受付装置から送信されてくるデータを受信する第 2 の受信手段と、第 2 の受信手段が受信した暗号化された第 1 の鍵を復号する第 1 の鍵復号手段と、復号された第 1 の鍵を用いて、第 2 の受信手段が受信した 2 重に暗号化された商品の発注内容を、部分的に復号する第 1 の発注内容復号手段と、部分的に復号された商品の発注内容に、第 1 の仮名情報とは異なる第 2 の仮名情報を付加して、商品発送装置に送信する第 3 の送信手段と、第 1 の仮名情報と第 2 の仮名情報との対応関係を記憶する第 2 の対応関係記憶手段とを含み、商品発送装置は、中継装置から送信されてくるデータを受信する第 3 の受信手段と、第 3 の受信手段が受信した暗号化された第 2 の鍵を復号する第 2 の鍵復号手段と、復号された第 2 の鍵を用いて、第 3 の受信手段が受信した部分的に復号された商品の発注内容を全面的に復号する第 2 の発注内容復号手段と、電子的商品を保管する商品保管手段と、全面的に復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、読み出し手段により読み出された電子的商品を、復号された第 2 の鍵を用いて暗号化する第 1 の商品暗号化手段と、第 2 の鍵を用いて暗号化された電子的商品を、第 3 の受信手段が受信した第 2 の仮名情報と共に、中継装置に送信する第 4 の送信手段とを含み、中継装置は、さらに商品発送装置から送信されてくるデータを受信する第 4 の受信手段と、第 4 の受信手段が受信した暗号化された電子的商品を、対応する第 1 の鍵を用いて 2 重に暗号化する第 2 の商品暗号化手段と、第 4 の受信手段が受信した第 2 の仮名情報に基づいて、第 2 の対応関係記憶手段を検索し、当該第 2 の仮名情報に対応する第 1 の仮名情報を特定する仮名情報特定手段と、第 2 の鍵を用いて 2 重に暗号化された電子的商品を、仮名情報特定手段により特定された第 1 の仮名情報と共に、受付装置に送信する第 5 の送信手段とを含み、受付装置は、さ

らに中継装置から送信されてくるデータを受信する第5の受信手段と、第5の受信手段が受信した第1の仮名情報に基づいて、第1の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、第5の受信手段が受信した2重に暗号化された電子的商品を、発注者特定手段により特定された発注者の物品購入装置に送信する第6の送信手段とを含み、物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含んでいる。

【0014】請求項4に係る発明は、請求項3の発明において、第1および第2の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【0015】請求項5に係る発明は、複数の発注者、受付部門、 n 個 (n は2以上の整数)の中継部門、商品部門を結ぶ通信ネットワークを用いて、電子的商品の発注と流通を行う通信販売システムであって、発注者、受付部門、中継部門および商品部門には、それぞれ、物品購入装置、受付装置、中継装置および商品発送装置が設けられており、物品購入装置は、電子データから成る第1および第2の鍵を発生する鍵発生手段と、第1および第2の鍵を用いて、商品の発注内容を2重に暗号化する発注内容暗号化手段と、第1および第2の鍵を、それぞれ別個に暗号化する鍵暗号化手段と、2重に暗号化された商品の発注内容に、暗号化された第1および第2の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する第1の送信手段とを含み、受付装置は、物品購入装置から送信されてくるデータを受信する第1の受信手段と、第1の受信手段が受信した本人確認情報が、正当なものか否かを確認する確認手段と、確認手段によって本人確認情報が正当なものと確認された場合、第1の受信手段が受信した2重に暗号化された商品の発注内容と、暗号化された第1および第2の鍵とに、発注者の識別情報とは異なる第1の仮名情報を付加して、第1番目の中継部門に属する中継装置に送信する第2の送信手段と、発注者の識別情報と第1の仮名情報との対応関係を記憶する第1の対応関係記憶手段とを含み、第1番目の中継部門に属する中継装置は、受付装置から送信されてくるデータを受信する第2の受信手段と、第2の受信手段が受信した暗号化された第1の鍵を復号する第1の鍵復号手段と、復号された第1の鍵を用いて、第2の受信手段が受信した2重に暗号化された商品の発注内容を、部分的に復号する第1の発注内容復号手段と、部分的に復号された商品の発注内容に、第1の仮名情報とは異なる第2の仮名情報を付加して、第2番目の中継装置に属する中継装置に送信する第3の送信手段と、第1の仮名情報と第2の仮名情報との対応関係を記憶する第2の対応関係記憶手段とを含み、第 m 番目 (m は、 $2 \leq m \leq n-1$ の整数)の中継部門に属する中継装置は、第 $(m-1)$ 番目の中継部門に属する中継装置から送信されてくるデータを受信する第3の受信手段

と、第3の受信手段が受信した部分的に復号された商品の発注内容に、第 m の仮名情報とは異なる第 $(m-1)$ の仮名情報を付加して、第 $(m-1)$ 番目の中継部門に属する中継装置に送信する第4の送信手段と、第 m の仮名情報と第 $(m+1)$ の仮名情報との対応関係を記憶する第3の対応関係記憶手段とを含み、第 n 番目の中継部門に属する中継装置は、第 $(n-1)$ 番目の中継部門に属する中継装置から送信されてくるデータを受信する第4の受信手段と、第4の受信手段が受信した部分的に復号された商品の発注内容に、第 n の仮名情報とは異なる第 $(n+1)$ の仮名情報を付加して、商品発送装置に送信する第5の送信手段と、第 n の仮名情報と第 $(n+1)$ の仮名情報との対応関係を記憶する第4の対応関係記憶手段とを含み、商品発送装置は、第 n 番目の中継部門に属する中継装置から送信されてくるデータを受信する第5の受信手段と、第5の受信手段が受信した暗号化された第2の鍵を復号する第2の鍵復号手段と、復号された第2の鍵を用いて、第5の受信手段が受信した部分的に復号された商品の発注内容を全面的に復号する第2の発注内容復号手段と、電子的商品を保管する商品保管手段と、全面的に復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出す読み出し手段と、読み出し手段により読み出された電子的商品を、復号された第2の鍵を用いて暗号化する第1の商品暗号化手段と、第2の鍵を用いて暗号化された電子的商品を、第5の受信手段が受信した第 $(n+1)$ の仮名情報と共に、第 n 番目の中継部門に属する中継装置に送信する第6の送信手段とを含み、第 n 番目の中継部門に属する中継装置は、さらに商品発送装置から送信されてくるデータを受信する第6の受信手段と、第6の受信手段が受信した第 $(n-1)$ の仮名情報に基づいて、第4の対応関係記憶手段を検索し、当該第 $(n+1)$ の仮名情報に対応する第 n の仮名情報を特定する第1の仮名情報特定手段と、第6の受信手段が受信した暗号化された電子的商品を、仮名情報特定手段により特定された第 n の仮名情報と共に、第 m 番目の中継部門に属する中継装置に送信する第7の送信手段とを含み、第 m 番目の中継部門に属する中継装置は、さらに第 $(m+1)$ 番目の中継部門に属する中継装置から送信されてくるデータを受信する第7の受信手段と、第7の受信手段が受信した第 m の仮名情報に基づいて、第3の対応関係記憶手段を検索し、当該第 m の仮名情報に対応する第 $(m-1)$ の仮名情報を特定する第2の仮名情報特定手段と、第7の受信手段が受信した暗号化された電子的商品を、仮名情報特定手段により特定された第 $(m-1)$ の仮名情報と共に、第 $(m-1)$ 番目の中継部門に属する中継装置に送信する第8の送信手段とを含み、第1番目の中継部門に属する中継装置は、さらに第2番目の中継部門に属する中継装置から送信されてくるデータを受信する第8の受信手段と、第8の受信手段が受信した暗

号化された電子的商品を、対応する第 1 の暗号鍵を用いて 2 重に暗号化する第 2 の商品暗号化手段と、第 8 の受信手段が受信した第 2 の仮名情報に基づいて、第 3 の対応関係記憶手段を検索し、当該第 2 の仮名情報に対応する第 1 の仮名情報を特定する第 3 の仮名情報特定手段と、第 8 の受信手段が受信した暗号化された電子的商品を、仮名情報特定手段により特定された第 1 の仮名情報と共に、受付装置に送信する第 9 の送信手段とを含み、受付装置は、さらに第 1 番目の中継部門に属する中継装置から送信されてくるデータを受信する第 9 の受信手段と、第 9 の受信手段が受信した第 1 の仮名情報に基づいて、第 1 の対応関係記憶手段を検索することにより、対応する発注者を特定する発注者特定手段と、第 9 の受信手段が受信した 2 重に暗号化された電子的商品を、発注者特定手段により特定された発注者の物品購入装置に送信する第 6 の送信手段とを含み、物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する手段をさらに含んでいる。

【0016】請求項 6 に係る発明は、複数の発注者、受付部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、発注者においては、電子データから成る鍵を発生する鍵発生ステップと、鍵を用いて、商品の発注内容を暗号化する発注内容暗号化ステップと、鍵を暗号化する鍵暗号化ステップと、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報を付加して、受付装置に送信する第 1 の送信ステップとを実行し、受付部門においては、発注者から送信されてくるデータを受信する第 1 の受信ステップと、第 1 の受信ステップで受信した本人確認情報が、正当なものか否かを確認する確認ステップと、確認ステップによって本人確認情報が正当なもの確認された場合、第 1 の受信ステップで受信した暗号化された商品の発注内容と暗号化された鍵とに、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する第 2 の送信ステップと、発注者の識別情報と仮名情報との対応関係を記憶する対応関係記憶ステップとを実行し、商品部門においては、受付部門から送信されてくるデータを受信する第 2 の受信ステップと、第 2 の受信ステップで受信した暗号化された鍵を復号する鍵復号ステップと、復号された鍵を用いて、第 2 の受信ステップで受信した暗号化された商品の発注内容を復号する発注内容復号ステップと、復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が受付部門にわからないように梱包封印する梱包封印ステップと、梱包封印された商品を、第 2 の受信ステップで受信した仮名情報と共に、受付部門に発送する第 1 の発送ステップとを実行し、受付部門においては、さらに商品部門から受け取った仮名情報に基づいて、対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ス

テップと、商品部門から受け取った梱包封印された商品を、発注者特定ステップで特定された発注者に発送する第 2 の発送ステップとを実行することを特徴とする。

【0017】請求項 7 に係る発明は、請求項 6 の発明において、仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【0018】請求項 8 に係る発明は、複数の発注者、受付部門、中継部門、商品部門を結ぶ通信ネットワークを用いて、実体的商品の発注と流通を行う通信販売方法であって、発注者においては、電子データから成る第 1 および第 2 の鍵を発生する鍵発生ステップと、第 1 および第 2 の鍵を用いて、商品の発注内容を 2 重に暗号化する発注内容暗号化ステップと、第 1 および第 2 の鍵を、それぞれ別個に暗号化する鍵暗号化ステップと、2 重に暗号化された商品の発注内容に、暗号化された第 1 および第 2 の鍵と、発注者の識別情報と、本人確認情報を付加して、受付装置に送信する第 1 の送信ステップとを含み、受付部門においては、物品購入装置から送信されてくるデータを受信する第 1 の受信ステップと、第 1 の受信ステップで受信した本人確認情報が、正当なものか否かを確認する確認ステップと、確認ステップによって本人確認情報が正当なもの確認された場合、第 1 の受信ステップで受信した 2 重に暗号化された商品の発注内容と暗号化された第 1 および第 2 の鍵とに、発注者の識別情報とは異なる第 1 の仮名情報を付加して、中継装置に送信する第 2 の送信ステップと、発注者の識別情報と第 1 の仮名情報との対応関係を記憶する第 1 の対応関係記憶ステップとを実行し、中継部門においては、受付装置から送信されてくるデータを受信する第 2 の受信ステップと、第 2 の受信ステップで受信した暗号化された第 1 の鍵を復号する第 1 の鍵復号ステップと、復号された第 1 の鍵を用いて、第 2 の受信ステップで受信した 2 重に暗号化された商品の発注内容を、部分的に復号する第 1 の発注内容復号ステップと、部分的に復号された商品の発注内容に、第 1 の仮名情報とは異なる第 2 の仮名情報を付加して、商品発送装置に送信する第 3 の送信ステップと、第 1 の仮名情報と第 2 の仮名情報との対応関係を記憶する第 2 の対応関係記憶ステップとを実行し、商品部門においては、中継装置から送信されてくるデータを受信する第 3 の受信ステップと、第 3 の受信ステップで受信した暗号化された第 2 の鍵を復号する第 2 の鍵復号ステップと、復号された第 2 の鍵を用いて、第 3 の受信ステップで受信した部分的に復号された商品の発注内容を全面的に復号する第 2 の発注内容復号ステップと、全面的に復号された商品の発注内容に基づいて、対応する商品を特定し、その内容が受付部門にわからないように梱包封印する第 1 の梱包封印ステップと、梱包封印された商品を、第 2 の受信ステップで受信した仮名情報と共に、中継部門に発送する第 1 の発送ステップとを実行し、中継部門においては、さらに商品部門から受け取っ

た梱包封印された商品を、さらに2重に梱包封印する第2の梱包封印ステップと、商品部門から受け取った第2の仮名情報に基づいて、第2の対応関係記憶ステップで記憶した対応関係を検索し、当該第2の仮名情報に対応する第1の仮名情報を特定する仮名情報特定ステップと、2重に梱包封印された商品を、仮名情報特定ステップにより特定された第1の仮名情報と共に、受付部門に発送する第2の発送ステップとを実行し、受付部門においては、さらに中継部門から受け取った第1の仮名情報に基づいて、第1の対応関係記憶ステップで記憶した対応関係を検索することにより、対応する発注者を特定する発注者特定ステップと、中継部門から受け取った2重に梱包封印された商品を、発注者特定ステップにより特定された発注者に発送する第3の発送ステップとを実行することを特徴とする。

【0019】請求項9に係る発明は、請求項8の発明において、第1および第2の仮名情報としては、各注文毎に異なる情報が使用されることを特徴とする。

【0020】

【作用】請求項1に係る発明においては、発注者、受付部門および商品部門は、相互に通信ネットワークで結ばれており、物品購入装置、受付装置および商品発送装置がそれぞれ設けられている。物品購入装置は、電子データから成る鍵を発生し、当該鍵を用いて商品の発注内容を暗号化する。また、当該鍵を暗号化する。さらに、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付装置は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した暗号化された商品の発注内容および暗号化された鍵に、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する。また、発注者の識別情報と仮名情報との対応関係を対応関係記憶手段に記憶する。商品発送装置は、受付装置から受信した暗号化された鍵を復号し、当該復号された鍵を用いて、受付装置から受信した暗号化された商品の発注内容を復号する。また、復号された商品の発注内容に基づいて、対応する電子的商品を商品保管手段から読み出し、この読み出した電子的商品を、復号された鍵を用いて暗号化し、仮名情報と共に、受付装置に送信する。受付装置は、さらに商品発送装置から受信した仮名情報に基づいて、対応関係記憶手段を検索し、対応する発注者を特定する。そして、暗号化された電子的商品を、特定された発注者の物品購入装置に送信する。物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する。

【0021】請求項2に係る発明においては、仮名情報として、各注文毎に異なる情報を使用することにより、プライバシーの機密性をより一層向上させている。

【0022】請求項3に係る発明においては、発注者、

受付部門、中継部門および商品部門は、相互に通信ネットワークで結ばれており、物品購入装置、受付装置、中継装置および商品発送装置がそれぞれ設けられている。物品購入装置は、電子データから成る第1および第2の鍵を発生し、当該第1および第2の鍵を用いて、商品の発注内容を2重に暗号化する。また、第1および第2の鍵を、それぞれ別個に暗号化する。さらに、2重に暗号化された商品の発注内容に、暗号化された第1および第2の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付装置は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した2重に暗号化された商品の発注内容と暗号化された第1および第2の鍵とに、発注者の識別情報とは異なる第1の仮名情報を付加して、中継装置に送信する。また、発注者の識別情報と第1の仮名情報との対応関係を第1の対応関係記憶手段に記憶する。中継装置は、受付装置から受信した暗号化された第1の鍵を復号し、この復号された第1の鍵を用いて、受付装置から受信した2重に暗号化された商品の発注内容を、部分的に復号する。また、部分的に復号された商品の発注内容に、第1の仮名情報とは異なる第2の仮名情報を付加して、商品発送装置に送信する。さらに、第1の仮名情報と第2の仮名情報との対応関係を第2の対応関係記憶手段に記憶する。商品発送装置は、中継装置から受信した暗号化された第2の鍵を復号し、この復号された第2の鍵を用いて、中継装置から受信した部分的に復号された商品の発注内容を全面的に復号する。また、全面的に復号された商品の発注内容に基づいて、商品保管手段を検索し、対応する電子的商品を読み出し、この読み出した電子的商品を、復号された第2の鍵を用いて暗号化する。さらに、第2の鍵を用いて暗号化された電子的商品を、第3の受信手段が受信した第2の仮名情報と共に、中継装置に送信する。中継装置は、さらに商品発送装置から受信した暗号化された電子的商品を、対応する第1の鍵を用いて2重に暗号化する。また、商品発送装置から受信した第2の仮名情報に基づいて、第2の対応関係記憶手段を検索し、当該第2の仮名情報に対応する第1の仮名情報を特定する。さらに、2重に暗号化された電子的商品を、特定された第1の仮名情報と共に、受付装置に送信する。受付装置は、さらに中継装置から受信した第1の仮名情報に基づいて、第1の対応関係記憶手段を検索し、対応する発注者を特定する。また、中継装置から受信した2重に暗号化された電子的商品を、特定された発注者の物品購入装置に送信する。物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する。

【0023】請求項4に係る発明においては、第1および第2の仮名情報として、各注文毎に異なる情報を使用することにより、プライバシーの機密性をより一層向上させている。

【0024】請求項5に係る発明においては、複数の発注者、受付部門、 n 個 (n は2以上の整数)の中継部門、商品部門は、通信ネットワークを用いて相互に結ばれており、物品購入装置、受付装置、中継装置および商品発送装置がそれぞれ設けられている。物品購入装置は、電子データから成る第1および第2の鍵を発生し、この第1および第2の鍵を用いて、商品の発注内容を2重に暗号化する。また、第1および第2の鍵を、それぞれ別個に暗号化する。さらに、2重に暗号化された商品の発注内容に、暗号化された第1および第2の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付装置は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した2重に暗号化された商品の発注内容と、暗号化された第1および第2の鍵と共に、発注者の識別情報とは異なる第1の仮名情報を付加して、第1番目の中継部門に属する中継装置に送信する。また、発注者の識別情報と第1の仮名情報との対応関係を第1の対応関係記憶手段に記憶する。第1番目の中継部門に属する中継装置は、受付装置から受信した暗号化された第1の鍵を復号し、この復号された第1の鍵を用いて、受付装置から受信した2重に暗号化された商品の発注内容を、部分的に復号する。また、部分的に復号された商品の発注内容に、第1の仮名情報とは異なる第2の仮名情報を付加して、第2番目の中継装置に属する中継装置に送信する。さらに、第1の仮名情報と第2の仮名情報との対応関係を第2の対応関係記憶手段に記憶する。第 m 番目 (m は、 $2 \leq m \leq n-1$ の整数)の中継部門に属する中継装置は、第 $(m-1)$ 番目の中継部門に属する中継装置から受信した部分的に復号された商品の発注内容に、第 m の仮名情報とは異なる第 $(m+1)$ の仮名情報を付加して、第 $(m+1)$ 番目の中継部門に属する中継装置に送信する。また、第 m の仮名情報と第 $(m+1)$ の仮名情報との対応関係を第3の対応関係記憶手段に記憶する。第 n 番目の中継部門に属する中継装置は、第 $(n-1)$ 番目の中継部門に属する中継装置から受信した部分的に復号された商品の発注内容に、第 n の仮名情報とは異なる第 $(n+1)$ の仮名情報を付加して、商品発送装置に送信する。また、第 n の仮名情報と第 $(n+1)$ の仮名情報との対応関係を第4の対応関係記憶手段に記憶する。商品発送装置は、第 n 番目の中継部門に属する中継装置から受信した暗号化された第2の鍵を復号し、この復号された第2の鍵を用いて、第 n 番目の中継部門に属する中継装置から受信した部分的に復号された商品の発注内容を全面的に復号する。また、全面的に復号された商品の発注内容に基づいて、商品保管手段から対応する電子的商品を読み出し、この読み出した電子的商品を、復号された第2の鍵を用いて暗号化する。さらに、第2の鍵を用いて暗号化された電子的商品を、第 n 番目の中継部門に属する中継装置から受

信した第 $(n-1)$ の仮名情報と共に、第 n 番目の中継部門に属する中継装置に送信する。第 n 番目の中継部門に属する中継装置は、さらに商品発送装置から受信した第 $(n-1)$ の仮名情報に基づいて、第4の対応関係記憶手段を検索し、当該第 $(n+1)$ の仮名情報に対応する第 n の仮名情報を特定する。また、商品発送装置から受信した暗号化された電子的商品を、特定された第 n の仮名情報と共に、第 m 番目の中継部門に属する中継装置に送信する。第 m 番目の中継部門に属する中継装置は、さらに第 $(m+1)$ 番目の中継部門に属する中継装置から受信した第 m の仮名情報に基づいて、第3の対応関係記憶手段を検索し、当該第 m の仮名情報に対応する第 $(m-1)$ の仮名情報を特定する。また、第 $(m-1)$ 番目の中継部門に属する中継装置から受信した暗号化された電子的商品を、特定された第 $(m-1)$ の仮名情報と共に、第 $(m-1)$ 番目の中継部門に属する中継装置に送信する。第1番目の中継部門に属する中継装置は、さらに第2番目の中継部門に属する中継装置から受信した暗号化された電子的商品を、対応する第1の暗号鍵を用いて2重に暗号化する。また、第2番目の中継部門に属する中継装置から受信した第2の仮名情報に基づいて、第3の対応関係記憶手段を検索し、当該第2の仮名情報に対応する第1の仮名情報を特定する。さらに、第2番目の中継部門に属する中継装置から受信した暗号化された電子的商品を、特定された第1の仮名情報と共に、受付装置に送信する。受付装置は、さらに第1番目の中継部門に属する中継装置から受信した第1の仮名情報に基づいて、第1の対応関係記憶手段を検索することにより、対応する発注者を特定する。また、第1番目の中継部門に属する中継装置から受信した2重に暗号化された電子的商品を、特定された発注者の物品購入装置に送信する。物品購入装置は、受付装置から送られてきた暗号化された電子的商品を復号する。

【0025】請求項6に係る発明においては、複数の発注者、受付部門、商品部門が、通信ネットワークを用いて互いに結ばれており、これらの中で実体的商品の発注と流通を行う。すなわち、発注者は、電子データから成る鍵を発生し、この鍵を用いて、商品の発注内容を暗号化する。また、鍵を暗号化する。さらに、暗号化された商品の発注内容に、暗号化された鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付部門は、発注者から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、発注者から受信した暗号化された商品の発注内容と暗号化された鍵と共に、発注者の識別情報とは異なる仮名情報を付加して、商品発送装置に送信する。また、発注者の識別情報と仮名情報との対応関係を記憶する。商品部門は、受付部門から受信した暗号化された鍵を復号し、この復号された鍵を用いて、受付部門から受信した暗号化された商品の発注内容を復号する。また、復号された商品の発注

内容に基づいて、対応する商品特定し、その内容が受付部門にわからないように梱包封印する。さらに、梱包封印された商品を、第2の受信ステップで受信した仮名情報と共に、受付部門に発送する。受付部門は、さらに商品部門から受け取った仮名情報に基づいて、対応する発注者を特定し、商品部門から受け取った梱包封印された商品を、特定された発注者に発送する。

【0026】請求項7に係る発明においては、仮名情報として、各注文毎に異なる情報を使用することにより、プライバシーの機密性をより一層向上させている。

【0027】請求項8に係る発明においては、複数の発注者、受付部門、中継部門、商品部門が、通信ネットワークを用いて互いに結ばれており、これら間で実体的商品の発注と流通を行う。すなわち、発注者は、電子データから成る第1および第2の鍵を発生し、この第1および第2の鍵を用いて、商品の発注内容を2重に暗号化する。また、第1および第2の鍵を、それぞれ別個に暗号化する。さらに、2重に暗号化された商品の発注内容に、暗号化された第1および第2の鍵と、発注者の識別情報と、本人確認情報とを付加して、受付装置に送信する。受付部門は、物品購入装置から受信した本人確認情報が、正当なものか否かを確認し、正当な場合は、物品購入装置から受信した2重に暗号化された商品の発注内容と暗号化された第1および第2の鍵とに、発注者の識別情報とは異なる第1の仮名情報を付加して、中継装置に送信する。また、発注者の識別情報と第1の仮名情報との対応関係を第1の対応関係記憶手段に記憶する。中継部門は、受付装置から受信した暗号化された第1の鍵を復号し、この復号された第1の鍵を用いて、受付装置から受信した2重に暗号化された商品の発注内容を、部分的に復号する。また、部分的に復号された商品の発注内容に、第1の仮名情報とは異なる第2の仮名情報を付加して、商品発送装置に送信する。さらに、第1の仮名情報と第2の仮名情報との対応関係を第2の対応関係記憶手段に記憶する。商品部門は、中継装置から受信した暗号化された第2の鍵を復号し、この復号された第2の鍵を用いて、中継装置から受信した部分的に復号された商品の発注内容を全面的に復号する。また、全面的に復号された商品の発注内容に基づいて、対応する商品特定し、その内容が受付部門にわからないように梱包封印する。さらに、梱包封印された商品を、中継装置から受信した仮名情報と共に、中継部門に発送する。中継部門は、さらに商品部門から受け取った梱包封印された商品を、さらに2重に梱包封印する。また、商品部門から受け取った第2の仮名情報に基づいて、対応する第1の仮名情報を特定し、2重に梱包封印された商品を、この特定された第1の仮名情報と共に、受付部門に発送する。受付部門は、さらに中継部門から受け取った第1の仮名情報に基づいて、対応する発注者を特定し、中継部門から受け取った2重に梱包封印された商品を、この特定さ

れた発注者に発送する。

【0028】請求項9に係る発明においては、第1および第2の仮名情報として、各注文毎に異なる情報が使用することにより、プライバシーの機密性をより一層向上させている。

【0029】

【実施例】図1は、本発明の一実施例に係る通信ネットワークを用いた通信販売システムの構成を示すブロック図である。図1において、本実施例のネットワークを用いた通信販売システムは、複数の発注者iと販売会社から成り立っている。販売会社は、受付部門a、中継部門b、商品部門cとに分かれており、各部門は独立に業務を遂行しており、各部門間で情報の公開は無いものとする。また、本システムに加入している発注者iには、各個人を識別できる発注者識別子IDiが付与されている。また、本実施例の通信ネットワークを用いた通信販売システムは、商品として、ゲームや業務用のソフトウェア、マルチメディア情報などの電子的商品を取り扱うものとする。

【0030】図1において、発注者iは、販売会社の受付部門aとパソコン通信でつながっていて、双方向に情報をやりとりする。受付部門aは、発注者iおよび中継部門bとパソコン通信でつながっていて、双方向に情報をやりとりする。中継部門bは、受付部門aおよび商品部門cとパソコン通信でつながっていて、双方向に情報をやりとりする。商品部門cは、中継部門bとパソコン通信でつながっていて、双方向に情報をやりとりする。

【0031】次に、図1に示す通信販売システムの概略的な動作を説明する。まず、発注者iは、欲しい商品の商品コードを二重に暗号化し、それを解読するための2つの暗号鍵をそれぞれ、中継部門b、商品部門c向けに暗号化する。そして、発注者iは、二重に暗号化された商品コードと、中継部門bおよび商品部門c向けに暗号化した暗号鍵とを合わせた暗号化発注内容を、発注者の識別子と共に、販売会社の受付部門aに送る。受付部門aは、発注者iから送られてきた情報、すなわち暗号化発注内容を、そのまま、照会番号(仮名情報)Ref1と共に、中継部門bに送る。中継部門bは、受付部門aから送られてきた暗号化発注内容の内、中継部門b向けに暗号化された暗号鍵を復号し、それを用いて二重に暗号化されている商品コードを一部復号する。そして、中継装置bは、一部復号された暗号化された商品コードと、商品部門c向けに暗号化された暗号鍵とを合わせて、照会番号Ref2と共に、商品部門cへ送る。商品部門cは、商品部門c向けに暗号化された暗号鍵を復号し、当該復号された暗号鍵を用いて、暗号化されている商品コードを復号する。これによって、発注されている商品名を知ることができる。

【0032】次に、商品部門cは、復号した商品コードに対応する商品そのものを暗号化し、当該暗号化された

商品を、その価格および照会番号 R e f 2 と共に、中継部門 b に送る。中継部門 b は、商品部門 c から送られてきた暗号化商品をさらに暗号化し、当該二重に暗号化された商品を、その価格および照会番号 R e f 1 と共に、受付部門 a に送る。受付部門 a は、照会番号 R e f 1 から発注者 i を対応づけ、商品の価格に等しい金額を発注者 i の銀行口座から引き落とし、また中継部門 b から送られてきた暗号化商品を、通信ネットワークを介して発注者 i に送る。発注者 i は、受付部門 a から送られてきた暗号化商品を復号し、発注した商品を手に入れる。

【0033】図2は、図1に示す発注者 i が所持している物品購入装置 10 の構成の一例を示すブロック図である。図2において、この物品購入装置 10 は、制御部 101 と、ROM 102 と、RAM 103 と、入力操作器 104 と、表示器 105 と、商品カタログ格納部 106 と、乱数発生部 107 と、秘密鍵保管部 108 と、通信部 109 と、発注データ格納部 110 とを備えている。

【0034】ROM 102 には、プログラムデータと、受付部門 a の公開鍵、中継部門 b の公開鍵、商品部門 c の公開鍵が格納され、制御部 101 は、このプログラムデータに従って動作する。RAM 103 は、制御部 101 の動作に必要な種々のデータを記憶する。入力操作器 104 は、発注者によって操作されるキーボードやマウス等を含み、制御部 101 に種々のデータや指示を入力する。表示器 105 は、CRT ディスプレイや液晶表示器によって構成され、制御部 101 から与えられる画像データを表示する。商品カタログ格納部 106 は、受付部門 a から定期的に送られてくる電子的な画像データを含む商品カタログを格納する。乱数発生部 107 は、発注内容の暗号化に必要な 2 つの乱数を生成する。秘密鍵保管部 108 は、発注者 i 固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部 109 は、受付部門 a とパソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部 110 は、商品発注データをやりとりする際に必要なデータを記憶している。

【0035】図3は、図1に示す受付部門 a に設けられている受付装置 20 の構成の一例を示すブロック図である。図3において、この受付装置 20 は、制御部 201 と、ROM 202 と、RAM 203 と、個人データ格納部 204 と、秘密鍵保管部 205 と、通信部 206 と、発注データ格納部 207 と、照会番号発行部 208 とを備えている。

【0036】ROM 202 には、プログラムデータならびに中継部門 b の公開鍵が格納され、制御部 201 は、このプログラムデータに従って動作する。RAM 203 は、制御部 201 の動作に必要な種々のデータを記憶する。個人データ格納部 204 には、本システムに加入している全ユーザの公開鍵、パソコン通信アドレス、銀行口座などの個人情報が、個人識別子と組にされて保管さ

れている。秘密鍵保管部 205 は、受付部門 a 固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部 206 は、各発注者および中継部門 b と、パソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部 207 は、商品発注データをやりとりをする際に必要なデータを記憶している。照会番号発行部 208 は、商品発注データのやりとりをする際に必要な照会番号を発行する。

【0037】図4は、図1に示す中継部門 b に設けられている中継装置 30 の構成の一例を示すブロック図である。図4において、この受付装置 30 は、制御部 301 と、ROM 302 と、RAM 303 と、秘密鍵保管部 304 と、通信部 305 と、発注データ格納部 306 と、照会番号発行部 307 とを備えている。

【0038】ROM 302 には、プログラムデータならびに受付部門 a の公開鍵が格納され、制御部 301 は、このプログラムデータに従って動作する。RAM 303 は、制御部 301 の動作に必要な種々のデータを記憶する。秘密鍵保管部 304 は、受付部門 b 固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部 305 は、受付部門 a と、商品部門 c と、パソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部 306 は、商品発注データをやりとりをする際に必要なデータを記憶している。照会番号発行部 307 は、商品発注データのやりとりをする際に必要な照会番号を発行する。

【0039】図5は、図1に示す商品部門 c に設けられた商品発送装置 40 の構成の一例を示すブロック図である。図5において、この商品発送装置 40 は、制御部 401 と、ROM 402 と、RAM 403 と、秘密鍵保管部 404 と、通信部 405 と、発注データ格納部 406 と、商品データ格納部 407 と、商品保管部 408 とを備えている。

【0040】ROM 402 には、プログラムデータならびに中継部門 b の公開鍵が格納され、制御部 401 は、このプログラムデータに従って動作する。RAM 403 は、制御部 401 の動作に必要な種々のデータを記憶する。秘密鍵保管部 404 は、受付部門 c 固有の秘密鍵を保管する。ただし秘密鍵は外部から読み出すことはできない。通信部 405 は、中継部門 b と、パソコン通信でつながっており、各入力されたデータを送受信する。発注データ格納部 406 は、商品発注データをやりとりをする際に必要なデータを記憶している。商品データ格納部 407 は、各商品の価格などが格納されている。商品保管部 408 は、商品部門 c が販売する全電子的商品が記録されている。ただし外部から読み出すことはできない。

【0041】図6は、図1に示す通信ネットワークを用いた通信販売システム全体の動作を示すシーケンスチャートである。図7は、図1の物品購入装置 10 の商品発

注時の動作を示すフローチャートである。図 8 は、図 1 の受付装置 20 の発注受付時の動作を示すフローチャートである。図 9 は、図 1 の中継装置 30 の発注中継時の動作を示すフローチャートである。図 10 は、図 1 の商品発送装置 40 の動作を示すフローチャートである。図 11 は、図 1 の中継装置 30 の商品中継時の動作を示すフローチャートである。図 12 は、図 1 の受付装置 20 の商品発送時の動作を示すフローチャートである。図 13 は、図 1 の物品購入装置 10 の商品受取時の動作を示すフローチャートである。以下、これら図 6 ~ 13 を参

照して、上記実施例の動作を説明する。

【0042】各発注者 i は、本システム加入時に、システム管理者に対して名前、パソコン通信アドレス、振替指定銀行口座などを書いたシステム加入申込書を送る。また同時に、振替指定銀行口座のある銀行に対して、銀行に受付部門 a から正当な料金振替請求があった場合には、銀行は発注者 i の許可なしで振り替えできる、という内容の契約書を送っておく。システム管理者は、発注者 i から送られてきたシステム加入申込書の内容の確認を行い、確認が取れた場合、発注者 i に個人識別子 ID_i と、発注者毎に異なりかつ秘密にしておく必要のある秘密鍵などを格納した物品購入装置 10 を配布（貸与、販売）する。また、システム管理者は、受付部門 a に、発注者 i の個人識別子 ID_i と、公開鍵 p_i と、振替指定口座とを組にして伝え、受付部門 a は、そのデータを図 1 の受付装置 10 内にある個人データ格納部 204（図 3 参照）に格納しておく。

【0043】システム管理者は、各発注者 i 、中継部門 b 、商品部門 c に対して、秘密鍵暗号アルゴリズム F と秘密鍵復号アルゴリズム F^{-1} を配布しておく。このとき、鍵 K を用いて秘密鍵暗号アルゴリズム F によりデータ X を暗号化した関数 $F(K, X)$ を復号できるのは、秘密鍵復号アルゴリズム F^{-1} と鍵 K の双方を保持しているものに限られる。すなわち、 $X = F^{-1}(K, F(K, X))$ が成立する。

【0044】次に、システム管理者は、各発注者 i に対して、公開鍵暗号アルゴリズム E と、中継部門 b および商品部門 c の公開鍵 p_b および p_c とを配布し、中継部門 b および商品部門 c に対して、公開鍵復号アルゴリズム D と、各自の秘密鍵 s_b および s_c とを配布する（公開鍵、秘密鍵は、商品部門毎に異なる）。このとき、 y （ y は、 b か c のいずれか）の公開鍵 p_y を用いて公開鍵暗号アルゴリズム E によりデータ X を暗号化した関数 $E(p_y, X)$ を復号できるのは、公開鍵復号アルゴリズム D と秘密鍵 s_y を保持しているものに限られる。すなわち、 $X = D(s_y, E(p_y, X))$ が成立する。また、秘密鍵 s_y は、 y しか知らない。また、各公開鍵 p_y から対応する秘密鍵 s_y は類推できな

い。

【0045】また、システム管理者は、各発注者 i 、受付部門 a 、中継部門 b 、商品部門 c に対して、署名生成アルゴリズム $sign$ および署名確認アルゴリズム $verify$ と、受付部門 a 、中継部門 b 、商品部門 c の公開鍵とを配布する（先に公開鍵暗号アルゴリズムの説明の時に述べた公開鍵・秘密鍵の値と同じである）。このとき、データ X に対して自分の秘密鍵 s_y （ y は、 i 、 a 、 b 、 c のいずれか）を用いて署名生成アルゴリズム $sign$ により作成した電子署名 $sign(s_y, X)$ は、秘密鍵 s_y を保持していないと作成できない。また、 y の公開鍵 p_y と署名確認アルゴリズム $verify$ とを用いることにより、電子署名 $sign(s_y, X)$ が、確かに y の作成したデータ X に対する電子署名であるか否かを確認できる。

【0046】各発注者 i 、受付部門 a 、中継部門 b 、商品部門 c においては、配布されたアルゴリズムと各公開鍵とが、各装置の内部にある ROM 102、202、302、402 にそれぞれ格納してある。また、各自の秘密鍵は、各装置内部の秘密鍵保管部 108、205、304、404 に保管され、外部からは読み出しできない。

【0047】なお、秘密鍵暗号アルゴリズム、公開鍵暗号アルゴリズム、署名生成アルゴリズムに関しては、「現代暗号理論」池野信一・小山謙二著（電子通信学会）に詳しく述べられているので、それを参照されたい。

【0048】以下の処理は、ある発注者 i が、商品コード PID の電子的商品 PDT を購入する場合の処理について述べている。

【0049】発注者 i には、定期的に受付部門 a から電子カタログが送付されてきて、商品カタログ格納部 106 に格納されている。発注者 i は、商品カタログ格納部 106 に格納されている電子カタログが、表示器 105 に表示されるのを見て、欲しいと思った商品があった場合、入力操作器 104 で画面をマークすることにより、購入商品を選択してその結果を制御部 101 に入力する（図 7 のステップ $S101$ ）。なお、購入商品の選択方法には、これ以外にも種々の方法（例えば、キー入力）を取り得ることを指摘しておく。次に、制御部 101 は、入力された購入商品に対応する商品コード PID を、商品カタログ格納部 106 から読みとる（ステップ $S102$ ）。

【0050】次に、制御部 101 は、乱数発生部 107 を用いて 2 つの乱数 r_b 、 r_c を発生する（ステップ $S103$ ）。次に、制御部 101 は、ROM 102 から秘密鍵暗号アルゴリズム F を読み込み、発生された乱数 r_b 、 r_c を鍵として、商品コード PID を次のように二重暗号化する（ステップ $S104$ ）。まず、 r_c を鍵として PID を暗号化する。

$F(r_c, PID)$

さらに、上記データ $F(r_c, PID)$ を、 r_b を鍵として暗号化する。

$F(r_b, F(r_c, PID))$

【0051】次に、制御部101は、ROM102から、公開鍵暗号アルゴリズムEと、中継部門bの公開鍵 p_b と、購入しようとしている商品を販売する商品部門cの公開鍵 p_c とを読み込み、下式(1)のように乱数 r_b を公開鍵 p_b を用いて公開鍵暗号アルゴリズムEに

$EOrd1 = F(r_b, F(r_c, PID)) \parallel$

$E(p_b, r_b) \parallel E(p_c, r_c) \dots (3)$

ただし、上式(3)において、 \parallel は情報の連結を表している。

【0053】次に、制御部101は、秘密鍵保管部108から発注者iの秘密鍵 s_i を、そしてROM102から署名生成アルゴリズム $sign$ を、それぞれ読み取り、下式(4)を用いて、 $EOrd1$ に対する電子署名を生成する(ステップS107)。

$sign(s_i, EOrd1) \dots (4)$

ここで、データXと、データXに対するyの電子署名 $sign(sy, X)$ の連結を、 $X[y]$ で簡単に表すことにする。すなわち、

$X[y] = X \parallel sign(sy, X)$

となる。

【0054】次に、制御部101は、個人識別子 ID_i と $EOrd1[i]$ とを、通信部109からパソコン通

$verify(p_i, sign(s_i, EOrd1)) \dots (5)$

制御部201は、電子署名の正当性が確認できれば、ステップS204へ進み、確認できない場合は、署名の正当性が確認できなかった旨を、通信部206を介して発注者iへ伝える(ステップS205)。

【0056】次に、制御部201は、照会番号発行部208を用いて照会番号 $Ref1$ を発行する(ステップS204)。次に、制御部201は、 $Ref1$ 、 ID_i 、 $EOrd1[i]$ を組にして、発注データ格納部207に格納する(ステップS206)。次に、制御部201は、ROM202から署名生成アルゴリズム $sign$ を、そして秘密鍵保管部205から秘密鍵 s_a を、それぞれ読み出し、次式(6)を用いて、照会番号 $Ref1$ に対する電子署名を生成する(ステップS207)。

$sign(s_a, Ref1) \dots (6)$

【0057】次に、制御部201は、 $Ref1[a]$ を受付番号として、発注者iに、通信部206からパソコン通信を用いて送信する(ステップS208)。

【0058】発注者iは、受付部門aから送られてきた $Ref1[a]$ と、暗号化発注内容 $EOrd1$ と、2つの乱数 r_b 、 r_c とを組にして、発注データ格納部11

$verify(p_a, sign(s_a, Ref1 \parallel EOrd1)) \dots (8)$

制御部301は、電子署名の正当性が確認できればステップS303へ進み、確認できない場合は、通信部30

より暗号化し、下式(2)のように乱数 r_c を公開鍵 p_c を用いて公開鍵暗号アルゴリズムEにより暗号化する(ステップS105)。

$E(p_b, r_b) \dots (1)$

$E(p_c, r_c) \dots (2)$

【0052】次に、制御部101は、 $F(r_b, F(r_c, PID))$ 、 $E(p_b, r_b)$ 、 $E(p_c, r_c)$ を連結して、下式(3)のように、暗号化発注内容 $EOrd1$ を生成する(ステップS106)。

信を用いて、受付部門aに送信する(ステップS108)。

【0055】受付部門aは、パソコン通信を用いて発注者iから送られてきたデータ ID_i と $EOrd1[i]$ とを、図3の通信部206を介して受信する(図8のステップS201)。次に、受付装置20の制御部201は、送られてきたデータの ID_i から対応する公開鍵 p_i を、個人データ格納部204から検索して、読み出す(ステップS202)。次に、制御部201は、ROM202から署名確認アルゴリズム $verify$ を読み出し、 $EOrd1[i]$ の電子署名 $sign(s_i, EOrd1)$ が $EOrd1$ に対する発注者iの電子署名であるか否かを、下式(5)を用いて確認する(ステップS203)。

0に保管する。

【0059】次に、受付部門aの制御部210は、照会番号 $Ref1$ と暗号化発注内容 $EOrd1$ とを連結したもののに対して、次式(7)を用いて、電子署名を施す(ステップS209)。

$sign(s_a, Ref1 \parallel EOrd1) \dots (7)$

次に、制御部201は、 $(Ref1 \parallel EOrd1)$

$[a]$ を、中継部門bに、通信部206からパソコン通信を用いて送信する(ステップS210)。

【0060】中継部門bは、パソコン通信を用いて受付部門aから送られてきたデータ $(Ref1 \parallel EOrd1)[a]$ を、図4の通信部305を介して受信する(図9のステップS301)。中継装置30の制御部301は、ROM302から、署名確認アルゴリズム $verify$ と、受付部門aの公開鍵 p_a とを読み出し、 $(Ref1 \parallel EOrd1)[a]$ の電子署名 $sign(s_a, Ref1 \parallel EOrd1)$ が、 $(Ref1 \parallel EOrd1)$ に対する受付部門aの電子署名であるか否かを、次式(8)を用いて確認する(ステップS302)。

5を介して受付部門aへ署名の正当性が確認できなかった旨を伝える(ステップS304)。

【0061】次に、制御部301は、EOrd1からE (pb, rb)を取り出し、秘密鍵保管部304から秘密鍵sbを、そしてROM302から公開鍵復号アルゴリズムDを読み込み、次式(9)に示すように、E (pb, rb)を鍵sbを用いてDにより復号し、rbを得る(ステップS303)。

$$D(sb, E(pb, rb)) = rb \quad \dots (9)$$

次に、制御部301は、ROM302から秘密鍵復号アルゴリズムF⁻¹を読み出し、次式(10)に示すよう

$$EOrd2 = F(rc, PID) \parallel E(pc, rc) \quad \dots (11)$$

【0063】次に、制御部301は、照会番号発行部307を用いて、照会番号Ref2を発行する(ステップS307)。次に、制御部301は、(Ref1 | EOrd1) [a]と、照会番号Ref2とを組にして、発注データ格納部306に格納する(ステップS30

$$sign(sb, Ref2 \parallel EOrd2) \quad \dots (12)$$

【0064】次に、制御部301は、(Ref2 | EOrd2) [b]を、商品部門cに、通信部305からパソコン通信を用いて送信する(ステップS310)。

【0065】商品部門cは、パソコン通信を用いて中継部門bから送られてきたデータ(Ref2 | EOrd2) [b]を、図5の通信部405を介して受信する(図10のステップS401)。商品発送装置40の制

$$verify(pb, sign(sb, Ref2 \parallel EOrd2)) \quad \dots (13)$$

制御部401は、電子署名の正当性が確認できればステップS403へ進み、確認できない場合は、通信部405を介して中継部門bへ署名の正当性が確認できなかった旨を伝える(ステップS404)。

【0066】次に、制御部401は、EOrd2からE (pc, rc)を取り出し、秘密鍵保管部404から秘密鍵scを、そしてROM402から公開鍵復号アルゴリズムDを読み込み、E (pc, rc)を鍵scを用い

$$F^{-1}(rc, F(rc, PID)) = PID \quad \dots (15)$$

次に、制御部401は、(Ref2 | EOrd2) [b]を、発注データ格納部406に格納する(ステップS406)。

【0067】次に、制御部401は、PIDの価格Prを商品データ格納部406から読み出し(ステップS407)、商品保管部408からPIDが対応する電子的商品PDTを取り出す(ステップS408)。次に、制御部401は、ROM402から秘密鍵暗号アルゴリズムFを読み込み、PDTを鍵rcを用いてFにより暗号

$$sign(sc, Ref2 \parallel EDPT1 \parallel Pr) \quad \dots (17)$$

【0069】次に、制御部401は、(Ref2 | EDPT1 | Pr) [c]を、中継部門bに、通信部405からパソコン通信を用いて送信する(ステップS411)。

【0070】中継部門bは、パソコン通信を用いて商品部門cから送られて来たデータ(Ref2 | EDPT1

に、EOrd1のF (rb, F (rc, PID))をrbを用いて一部だけ復号する(ステップS305)。

$$F^{-1}(rb, F(rb, F(rc, PID)))$$

$$= F(rc, PID) \quad \dots (10)$$

【0062】次に、制御部301は、F (rc, PID)とEOrd1のE (pc, rc)とを連結して、次式(11)で示されるEOrd2を生成する(ステップS306)。

7)。次に、制御部301は、ROM302から署名生成アルゴリズムsignを読み出し、Ref2とEOrd2とを連結したものに対して、次式(12)を用いて、電子署名を施す(ステップS309)。

制御部401は、ROM402から、署名確認アルゴリズムverifyと、中継部門bの公開鍵pbとを読み出し、(Ref2 | EOrd2) [b]の電子署名sign (sb, Ref2 | EOrd2)が、(Ref2 | EOrd2)に対する中継部門bの電子署名であるか否かを、次式(13)を用いて確認する(ステップS402)。

$$\dots (13)$$

てDにより復号し、次式(14)で示されるrcを得る(ステップS403)。

$$D(sc, E(pc, rc)) = rc \quad \dots (14)$$

次に、制御部401は、ROM402から秘密鍵復号アルゴリズムF⁻¹を読み出し、EOrd2のF (rc, PID)をrcだけを用いて次式(15)のように復号する(ステップS405)。

化することにより、次式(16)で示されるEPDT1を生成する(ステップS409)。

$$EPDT1 = F(rc, PDT) \quad \dots (16)$$

【0068】次に、制御部401は、ROM402から署名生成アルゴリズムsignを読み込み、Ref2、EDPT1、Prを連結したものに対して、次式(17)で示されるような電子署名を作成する(ステップS410)。

| Pr) [c]を、図4の通信部304を介して受信する(図11のステップS501)。中継装置30の制御部301は、ROM302から、署名確認アルゴリズムverifyと、商品部門cの公開鍵pcとを読み出し、(Ref2 | EDPT1 | Pr) [c]の電子署名sign (sc, Ref2 | EDPT1 | Pr)が、

(Ref 2 || EDPT1 | Pr) に対する商品部門 c の電子署名であるか否かを、次式 (18) を用いて確認す

$$\text{verify}(\text{pc}, \text{sign}(\text{sc}, \text{Ref 2 || EDPT1 || Pr}))$$

… (18)

制御部 401 は、電子署名の正当性が確認できればステップ S503 へ進み、確認できない場合は、通信部 305 を介して商品部門 c へ署名の正当性が確認できなかった旨を伝える (ステップ S504)。

【0071】次に、制御部 301 は、送られてきた (Ref 2 || EDPT1 || Pr) [c] に含まれている照会番号 Ref 2 に基づいて、発注データ格納部 306 を検索し、当該照会番号 Ref 2 と共に記録されている (R

$$\text{EPDT2} = \text{F}(\text{rb}, \text{EPDT1})$$

$$= \text{F}(\text{rb}, \text{F}(\text{rc}, \text{PDT})) \quad \dots (19)$$

【0073】次に、制御部 301 は、ROM302 から署名生成アルゴリズム sign を、秘密鍵保管部 304 から秘密鍵 sb を、それぞれ読み出し、照会番号 Ref 2 と共に記録されている (Ref 1 || EOrd1)

$$\text{sign}(\text{sb}, \text{Ref 1 || EPDT2 || Pr}) \quad \dots (20)$$

【0074】次に、制御部 301 は、商品部門 c から送られてきた (Ref 2 || EDPT1 || Pr) [c] を、(Ref 1 || EOrd1) [a] と組にして発注データ格納部 306 に格納する (ステップ S507)。次に、制御部 301 は、(Ref 1 || EPDT2 || Pr)

[b] を、受付部門 a に、通信部 305 からパソコン通信を用いて送信する (ステップ S508)。

【0075】受付部門 a は、パソコン通信を介して中継部門 b から送られてきたデータ (Ref 1 || EPDT2

$$\text{verify}(\text{pb}, \text{sign}(\text{sb}, \text{Ref 1 || EPDT2 || Pr}))$$

… (21)

制御部 201 は、電子署名の正当性が確認できればステップ S603 へ進み、確認できない場合は、通信部 206 を介して中継部門 b へ署名の正当性が確認できなかった旨を伝える (ステップ S604)。

【0076】次に、制御部 201 は、発注データ格納部 207 を検索して、中継部門 b から送られてきた (Ref 1 || EPDT2 || Pr) [b] から Ref 1 を取り出し、(Ref 1 || EPDT2 || Pr) [b] を、ID i

$$\text{sign}(\text{sa}, \text{Ref 1 || EPDT2 || Pr}) \quad \dots (22)$$

【0078】次に、制御部 201 は、照会番号 Ref 1 とともに発注データ格納部 207 に格納されている個人識別子 ID i を求め、そして当該 ID i に対応するパソコン通信アドレスを個人データ格納部 204 から検索し、発注者 i に、(Ref 1 || EPDT2 || Pr)

[a] を、通信部 206 からパソコン通信を用いて送信する (ステップ S606)。

【0079】発注者 i は、パソコン通信を介して受付部門 a から送られてきたデータ (Ref 1 || EPDT2 ||

$$\text{verify}(\text{pa}, \text{sign}(\text{sa}, \text{Ref 1 || EPDT2 || Pr}))$$

… (23)

る (ステップ S502)。

ef 1 || EOrd1) [a] から、図 9 のステップ S303 と同じようにして、乱数 rb を取り出す (ステップ S503)。

【0072】次に、制御部 301 は、ROM302 から秘密鍵暗号アルゴリズム F を読み出し、鍵 rb を用いて、EPDT1 を暗号化し、次式 (19) で示される EPDT2 を生成する (ステップ S505)。

[a] から取り出した照会番号 Ref 1 と、商品部門 c から送られてきた EPDT2 と Pr とを連結した (Ref 1 || EPDT2 || Pr) に対し、次式 (20) を用いて、電子署名を施す (ステップ S506)。

[b] を、図 3 の通信部 206 を介して受信する (図 12 のステップ S601)。受付装置 20 の制御部 201 は、ROM202 から、署名確認アルゴリズム verify と、中継部門 b の公開鍵 pb とを読み出し、(Ref 1 || EPDT2 || Pr) [b] の電子署名 sign(sb, Ref 1 || EPDT2 || Pr) が、(Ref 1 || EPDT2 || Pr) に対する中継部門 b の電子署名であるか否かを、次式 (21) を用いて確認する (ステップ S602)。

および EOrd1 [i] と組にして、発注データ格納部 207 に記録する (ステップ S603)。

【0077】次に、制御部 201 は、ROM202 から署名生成アルゴリズム sign を、秘密鍵保管部 205 から秘密鍵 sa を、それぞれ取り出し、Ref 1 || EPDT2 || Pr に対する電子署名を、次式 (22) を用いて生成する (ステップ S605)。

(Ref 1 || EPDT2 || Pr) [a] を、図 2 の通信部 109 を介して受信する (図 13 のステップ S701)。物品購入装置 10 の制御部 101 は、ROM102 から、署名確認アルゴリズム verify と、受付部門 a の公開鍵 pa とを読み出し、(Ref 1 || EPDT2 || Pr) [a] の電子署名 sign(sa, Ref 1 || EPDT2 || Pr) が、(Ref 1 || EPDT2 || Pr) に対する受付部門 a の電子署名であるか否かを、次式 (23) を用いて確認する (ステップ S702)。

制御部101は、電子署名の正当性が確認できればステップS703へ進み、確認できない場合は、通信部109を介して受付部門aへ署名の正当性が確認できなかった旨を伝える(ステップS704)。

【0080】次に、制御部101は、送られてきた(Ref1||EDPT2||Pr)[a]からRef1を取り出し、発注データ格納部110に格納されているRef1[a]を検索し、その中で発注した商品の価格と、送られてきた(Ref1||EDPT2||Pr)[a]のPrとが一致するかどうか確かめる(ステップS70

105)。

$$Receipt = sign(si, Ref1 || EDPT2 || Pr)$$

次に、制御部101は、商品受取票ReceiptをRef1と共に、通信部109からパソコン通信を用いて、受付部門aに送信する(ステップS707)。

【0082】次に、制御部101は、ROM102から秘密鍵復号アルゴリズムF⁻¹を読み出し、Ref1と組にして発注データ保管部に保管されている2つの乱数rb、rcを読み出す。そして、制御部101は、次式(25)のように、鍵rbをF⁻¹に代入することにより、EPDT2を復号し、EPDT1を得る(ステップS708)。

$F^{-1}(rb, EPDT2) = EPDT1$ … (25)

次に、制御部101は、鍵rcをF⁻¹に代入することにより、EPDT1を復号し、発注した電子的商品PDTを得る(ステップS709)。

$F^{-1}(rc, EPDT1) = PDT$ … (26)

【0083】なお、復号した商品PDTが発注したものと異なる場合は、制御部101は、パソコン通信を使って受付部門aに商品違いをアピールする(ステップS710)。

【0084】受付部門aにおいて、制御部201は、発注者i送られてきたRef1が発注データ格納部207に記録されているかどうかを検索し、発注者iから送られてきたReceiptを、Ref1と共に格納されているIDi、EOrd1[i]、(Ref1||EPDT2||Pr)と組にして保管する。そして、制御部201は、発注者iの予め登録されている振替指定銀行口座から、商品PDTの価格Prを引き落とし受付部門aの口座に振替えるように、銀行に依頼する。

【0085】次に、以上説明した通信ネットワークを用いた通信販売システムにおいて、「誰が何を買ったのか」わからない、というプライバシー保護が実現できていることについて述べる。まず初めに、受付部門a、中継部門b、商品部門cの3つ全てが結託しないと「誰が何を買った」という情報がわからないことを示す。その後、各手続きにおいて、発注者i、受付部門a、中継部門b、商品部門cが通常の手続きをしなかった場合の対策についても述べる。

【0086】図14は、先に説明した通信ネットワーク

3)。制御部101は、一致した場合は、ステップS705へ進み、一致しなかった場合は、通信部109を介して受付部門aへ値段が違っているとアピールする(ステップS706)。

【0081】制御部101は、ROM102から署名生成アルゴリズムsignを、秘密鍵保管部108から秘密鍵siを、それぞれ読み出し、Ref1||EDPT2||Prに対する電子署名を次式(24)を用いて生成し、商品受取票Receiptとする(ステップS70

105)。

$Receipt = sign(si, Ref1 || EDPT2 || Pr)$
… (24)

を用いた通信販売システムにおいて、受付部門a、中継部門b、商品部門cのそれぞれが、各手続きにおいて登場する情報のどれを知っているかを示している。○はその情報を保持していて、×は保持していないことを示している。

【0087】発注者iの個人識別子IDiは、受付部門aしか知らず、商品名PIDは商品部門cしか知らない。これは、商品に関する情報は、受付部門a、中継部門bでは暗号化された状態で処理されるからである。しかも、受付部門aと商品部門cが共有している情報は、商品の価格Prしかないもので、商品の価格がほとんど均一でしかも情報量が多いならば、仮に受付部門aと商品部門cが互いに自分の持つ情報を相手に渡したとしても、それぞれが保持する情報を結び付ける情報がない。すなわち「誰が何を買ったのか」がわからない。また、中継部門bには、商品に関する情報も、発注者iに関する情報も無いので、受付部門a、商品部門cのいずれかと、互いに自分の持つ情報を相手に渡したとしても、「誰が何を買ったのか」がわからない。したがって、「誰が何を買った」という情報がわかるためには、受付部門a、中継部門b、商品部門cの3つが結託し、互いに自分の持つ情報を相手に渡すことが必要となる。各部門が正常な組織倫理に基づいて運用される限り、3部門共が結託する可能性は非常に小さい。よって、「誰が何を買ったのかわからない」というプライバシー保護が実現できている。すなわち、発注者は匿名で通信ネットワークを介して商品を注文購入できる。

【0088】次に、各手続きにおいて、発注者i、受付部門a、中継部門b、商品部門c(以下、単にまとめてセクションと呼ぶ)が通常の手続きをしなかった場合の対策について述べる。ここで、通常の手続きをしないと、送られてきた情報を処理して次の手続きへ送る際に、情報を改ざんしたりすることである。たとえば、先に説明した通信ネットワークを用いた通信販売システムにおいて、受付部門aが発注者iから受け付けた暗号化発注内容EOrd1の内容の全部または一部を別のものにするといった場合がある。

【0089】各手続きにおいて、各セクションが、送ら

れてきた情報を書き替えて次の手続きへ送った場合は、各手続きにおいて情報を送る時に、そのセクションしか作成できない電子署名を一緒に送付している。電子署名は、送信途中で内容が改ざんされた場合でも署名確認時に判明する。すなわち、各セクションの発注データ格納部には、送られてきた情報とその電子署名が格納されているため、その情報を元にたどっていけば誰が情報を書き換えたかが判明する。したがって、各セクションは、情報を無断で書き換えることができない。

【0090】以上説明したように、上記実施例の通信ネットワークを用いた通信販売システムにおいては、「誰が何を買ったのかわからない」というプライバシー保護が実現できていて、発注者 i、受付部門 a、中継部門 b、商品部門 c のいずれかが通常の手続きをしなかった場合も、そのような手続きをどの部門で行ったかが特定できる。

【0091】なお、上記実施例においては、発注者 i、受付部門 a、中継部門 b、商品部門 c の双方向通信を、パソコン通信を用いて行なっているが、デジタル CATV 網、B-I SDN などの双方向通信が行なえる他の通信ネットワークを採用してもよく、この場合も上記実施例と同様の効果が得られる。

【0092】また、上記実施例においては、発注者 i から受付部門 a への商品代金の受渡しを、システム申込時に振替指定銀行口座をシステム管理者に知らせ、受付部門 a がその振替指定銀行口座から受付部門 a の口座へ振り替えてもらうように銀行に依頼することで実現しているが、システム加入時に予め発注者 i が加入しているクレジットカード部門の会員番号を知らせ、受付部門 a は商品代金を指定されたクレジットカード部門から立て替え払いしてもらうことで実現してもよく、この場合も上記実施例と同様の効果が得られる。

【0093】また、上記実施例においては、受付部門 a と商品部門 c との間に中継部門 b を設定しているが、中継部門を省略することもできる。この場合、受付部門 a は発注者が誰であるかを特定できるが、発注内容ならびに商品そのものは暗号化されているので何を買ったのかを特定できない。また、商品部門 c は、何を買ったのかは特定できるが、受付部門 a から送られてくる照会番号は発注者とは対応づけられない。すなわち、誰が買ったのかを特定できない。よって、この場合も、いずれの部門も、単独では「誰が何を買ったのか」がわからず、プライバシー保護が実現できている。

【0094】また、上記実施例においては、購入する商品を電子的商品としたが、電子的ではない一般的な商品に対しても、プライバシーを保護する本発明の通信ネットワークを用いた通信販売システムを適用することが可能である。ただし、この場合、上記実施例の手続きを若干手変更する必要がある。このことを以下に述べる。

【0095】発注者 i が商品を発注して、その発注情報

を受付部門 a が受け付けて、中継部門 b を介して、商品部門 c にパソコン通信を用いて送るところまでは同じである。しかしながら、電子的ではない一般的な商品は暗号化できないので、商品部門 c は、商品を物理的に包装した後、商品部門 c しか持っていない用紙で封印をして、当該封印された商品を Ref 2 と共に、中継部門 b に物理的に送る。中継部門 b では、送られてきた商品部門 c の封印のついた商品を、さらに包装し、中継部門 b しか持っていない用紙で封印する。そして、当該二重に封印された商品を、Ref 2 に対応する Ref 1 と共に受付部門 a に物理的に送る。受付部門 a は、二重に封印された商品を、発注者 i に物理的に届ける。また、上記実施例においては、商品部門 c から中継部門 b および受付部門 a を介して、発注者 i に商品を送付する際に、電子署名を付加して送信しているが、この点は、物品受領書と通常の印鑑に変わる。

【0096】上記のように、電子的ではない一般的な商品に対しても、プライバシーを保護する本発明の通信ネットワークを用いた通信販売システムを適用することが可能である。

【0097】また、上記実施例においては、中継部門を 1 つとして説明したが、中継部門を複数設けたシステム、すなわち第 1 ～第 n (n は 2 以上の整数) の中継部門を揺するシステムにも本発明を適用することが可能である。ただし、この場合、上記実施例の手続きを若干変更する必要があるので、以下にこのことを述べる。

【0098】上記実施例における中継部門 b は、第 1 の中継部門 b 1 が代わる。この時、第 1 の中継部門 b 1 から直接に商品部門 c に、

(Ref 2 || EOrd 2) [b 1]

を送るのではなく、第 2 の中継部門 b 2 から第 n の中継部門 b n を介して送られる。すなわち、第 m の中継部門 b m から第 (m+1) の中継部門 b (m+1) へは、

(Ref (m-1) || EOrd 2) [b m]

が送信される。ただし、Ref (m+1) は、第 (m+1) の照会番号である。また、Ref 1 から Ref (n+1) までは、各値がすべて異なる。そして、第 n の中継部門 b n から商品部門 c へは、

(Ref (n-1) || EOrd 2) [b n]

が送られる。商品部門 c では、受信した (Ref (n+1) || EOrd 2) [b n] から PID を得て、PDT を暗号化し、

(Ref (n-1) || EPDT 1 || Pr) [c]

を第 n の中継部門 b n へ送信する。また、第 m の中継部門 b m から第 (m-1) の中継部門 b (m-1) へは、

(Ref (m-1) || EPDT 1 || Pr) [b m]

が送信される。そして、第 1 の中継部門 b 1 から受付部門 a には、

(Ref 2 || EPDT 1 || Pr) [b 1]

が送信される。以下の手順は、上記実施例と同じであ

る。この場合のプライバシーの安全性は、上記実施例の安全性のところで述べたように、各部門の結託の可能性に依存しており、その可能性は上記実施例に比べて低くなる。

【0099】また、上記実施例では、受付部門 a、中継部門 b、商品部門 c を、1つの会社内に設けるようにしたが、これら各部門を別会社として組織するようにしてもよい。

【0100】

【発明の効果】請求項 1 の発明によれば、受付部門は、発注者の発注した商品の内容および商品部門から送られてくる電子的商品を、暗号化された状態でしか見ることができないので、いかなる商品が発注されたかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる仮名情報が付加されて送られてくるので、誰が商品が発注したかを知ることができない。したがって、受付部門と商品部門とが結託しない限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。また、発注者から

受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落としなどの既存の決済システムをそのまま使用することができる。

【0101】請求項 2 の発明によれば、仮名情報として、各注文毎に異なる情報を使用しているため、商品部門が仮名情報と発注者との対応関係を突き止めるような不正を有効に防止することができる。

【0102】請求項 3 の発明によれば、受付部門は、発注者の発注した商品の内容および中継部門から送られてくる電子的商品を、暗号化された状態でしか見ることができないので、いかなる商品が発注されたかを知ることができない。また、中継部門は、発注者の発注した商品の内容および商品部門から送られてくる電子的商品を、暗号化された状態でしか見ることができないので、いかなる商品が発注されたかを知ることができない。さらに、中継部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる第 1 の仮名情報が付加されて送られてくるので、誰が商品が発注したかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、第 1 の仮名情報とは異なる第 2 の仮名情報が付加されて送られてくるので、誰が商品が発注したかを知ることができない。したがって、受付部門と中継部門と商品部門とが結託しない限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。なお、受付部門と商品部門が結託しようとしても、両部門の持っている情報を結び付ける情報がないので、結託しようがない。したがって、結託によるプライバシーの侵害を有効に防止することができる。また、発注者から受付部門

に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落としなどの既存の決済システムをそのまま使用することができる。

【0103】請求項 4 の発明によれば、第 1 および第 2 の仮名情報として、各注文毎に異なる情報を使用しているため、中継部門または商品部門が仮名情報と発注者との対応関係を突き止めるような不正を有効に防止することができる。

【0104】請求項 5 の発明によれば、中継部門が複数設けられ、商品の発注内容および発注された商品がこれら複数の中継部門を介して伝達されるので、各部門の結託がより一層困難になり、発注者のプライバシーをより確実に保護することができる。

【0105】請求項 6 の発明によれば、受付部門は、発注者の発注した商品の内容を暗号化された状態でしか見ることができず、また商品部門から送られてくる実体的商品が封印梱包されているので、いかなる商品が発注されたかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる仮名情報が付加されて送られてくるので、誰が商品が発注したかを知ることができない。したがって、受付部門と商品部門とが結託しない限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。また、発注者から受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落としなどの既存の決済システムをそのまま使用することができる。

【0106】請求項 7 の発明によれば、仮名情報として、各注文毎に異なる情報を使用しているため、商品部門が仮名情報と発注者との対応関係を突き止めるような不正を有効に防止することができる。

【0107】請求項 8 の発明によれば、受付部門は、発注者の発注した商品の内容を暗号化された状態でしか見ることができず、また中継部門から送られてくる実体的商品が封印梱包されているので、いかなる商品が発注されたかを知ることができない。また、中継部門は、発注者の発注した商品の内容を暗号化された状態でしか見ることができず、また商品部門から送られてくる実体的商品が封印梱包されているので、いかなる商品が発注されたかを知ることができない。さらに、中継部門は、暗号化された商品の発注内容に、発注者の識別情報とは異なる第 1 の仮名情報が付加されて送られてくるので、誰が商品が発注したかを知ることができない。また、商品部門は、暗号化された商品の発注内容に、第 1 の仮名情報とは異なる第 2 の仮名情報が付加されて送られてくるので、誰が商品が発注したかを知ることができない。したがって、受付部門と中継部門と商品部門とが結託しない

限り、販売側では「誰が何を買ったのか」を把握することができず、結果として発注者のプライバシーを有効に保護することができる。なお、受付部門と商品部門が結託しようとしても、両部門の持っている情報を結び付ける情報がないので、結託しようがない。したがって、結託によるプライバシーの侵害を有効に防止することができる。また、発注者から受付部門に送られる商品の発注内容には、本人確認情報が付加されるため、受付部門で本人確認を行うことにより、クレジットカードや銀行引き落としなどの既存の決済システムをそのまま使用することができ

【0108】請求項9の発明によれば、中継部門が複数設けられ、商品の発注内容および発注された商品がこれら複数の中継部門を介して伝達されるので、各部門の結託がより一層困難になり、発注者のプライバシーをより確実に保護することができる。

【図面の簡単な説明】

【図1】本発明の一実施例に係る通信ネットワークを用いた通信販売システムの構成を示すブロック図である。

【図2】図1に示す発注者1に設けられた物品購入装置10の構成の一例を示すブロック図である。

【図3】図1に示す受付部門aに設けられた受付装置20の構成の一例を示すブロック図である。

【図4】図1に示す中継部門bに設けられた中継装置30の構成の一例を示すブロック図である。

【図5】図1に示す商品部門cに設けられた商品発送装置40の構成の一例を示すブロック図である。

【図6】図1に示す通信ネットワークを用いた通信販売システム全体の動作を示すシーケンスチャートである。

【図7】図1の物品購入装置10の商品発注時の動作を示すフローチャートである。

【図8】図1の受付装置20の発注受付時の動作を示すフローチャートである。

【図9】図1の中継装置30の発注中継時の動作を示すフローチャートである。

【図10】図1の商品発送装置40の動作を示すフローチャートである。

【図11】図1の中継装置30の商品中継時の動作を示すフローチャートである。

【図12】図1の受付装置20の商品発送時の動作を示すフローチャートである。

【図13】図1の物品購入装置10の商品受け取り時の動作を示すフローチャートである。

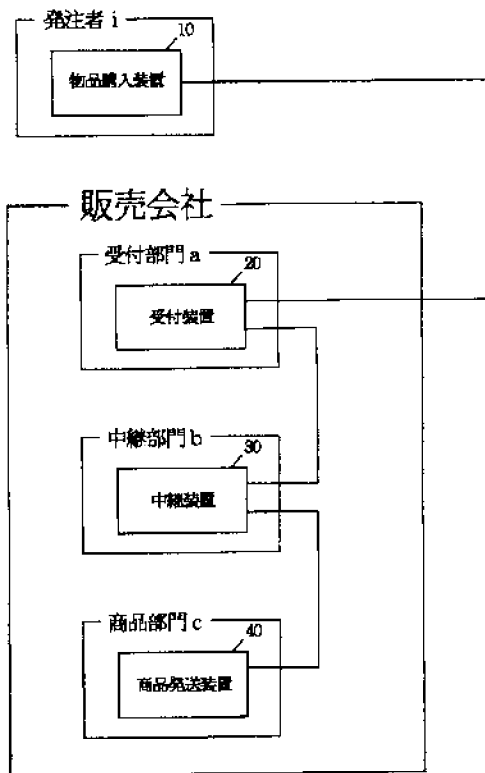
【図14】図1の実施例において、各部門で知り得る情報を説明するための図である。

【図15】従来の通信ネットワークを用いた通信販売システムの構成の一例を示すブロック図である。

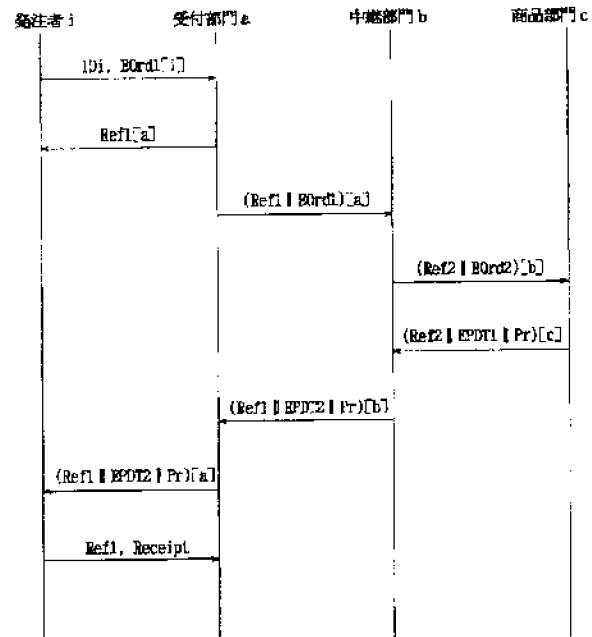
【符号の説明】

- 1…発注者
- 10…物品購入装置
- 2…受付部門
- 20…受付装置
- 3…中継部門
- 30…中継装置
- 4…商品部門
- 40…商品発送装置
- 101, 201, 301, 401…制御部
- 102, 202, 302, 402…ROM
- 103, 203, 303, 403…RAM
- 104…入力操作器
- 105…表示器
- 106…商品カタログ格納部
- 107…乱数発生部
- 108, 205, 304, 404…秘密鍵保管部
- 109, 206, 305, 405…通信部
- 110, 207, 306, 406…発注データ格納部
- 204…個人データ格納部
- 208, 307…照会番号発行部
- 407…商品データ格納部
- 408…商品保管部

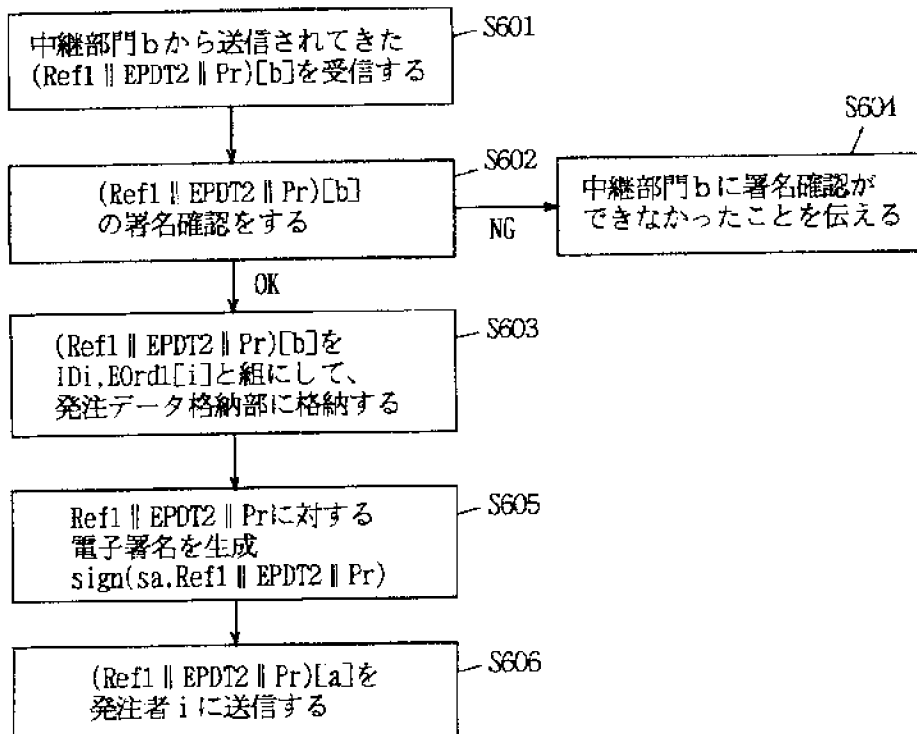
【図 1】



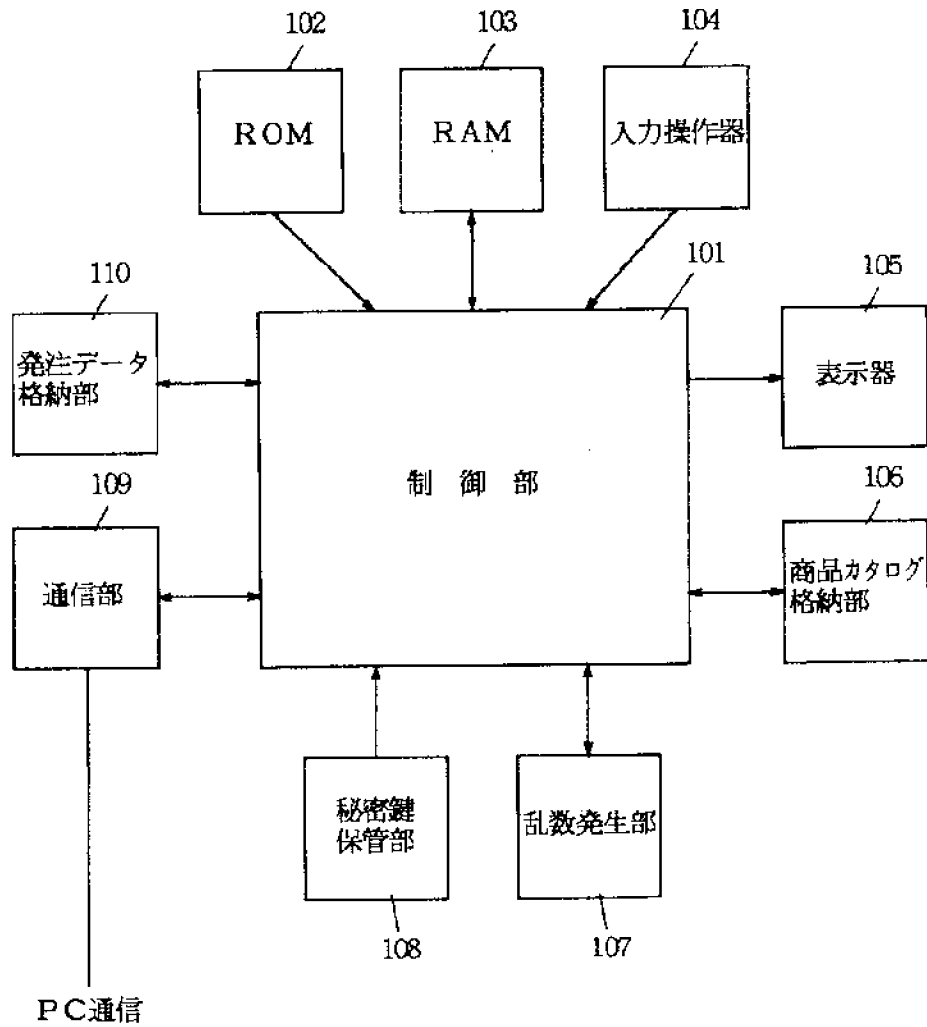
【図 6】



【図 12】



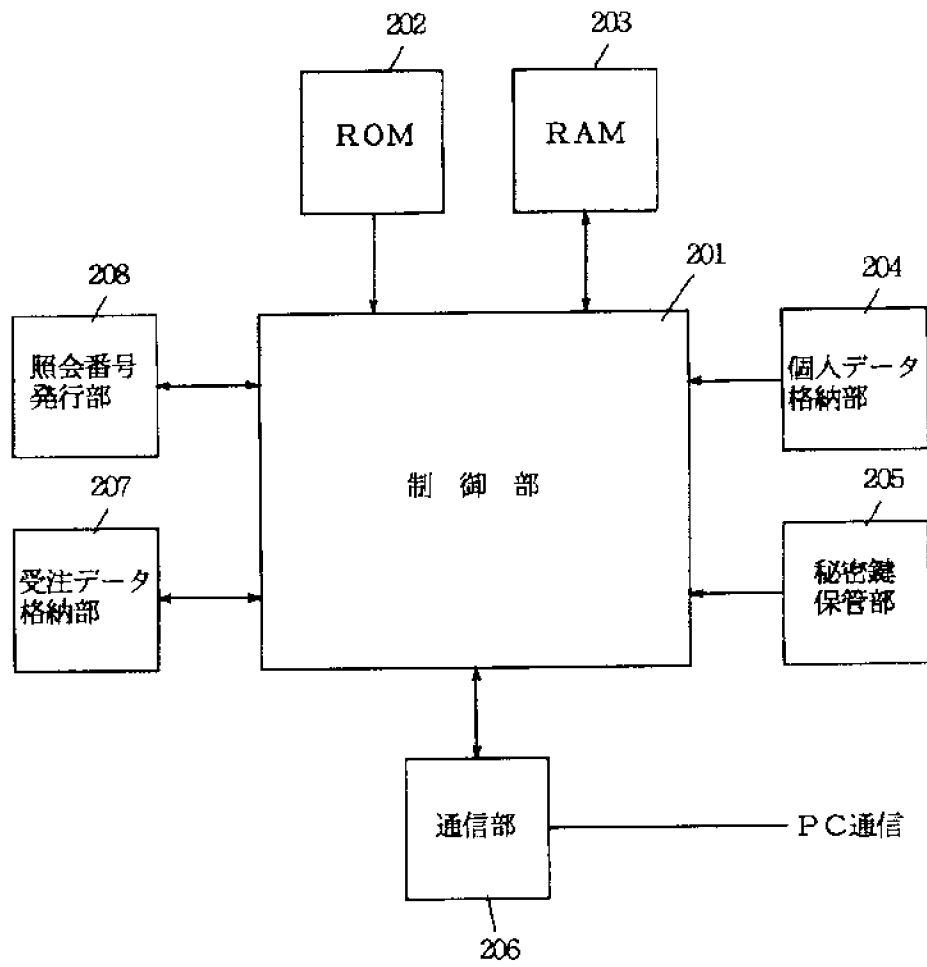
【図 2】



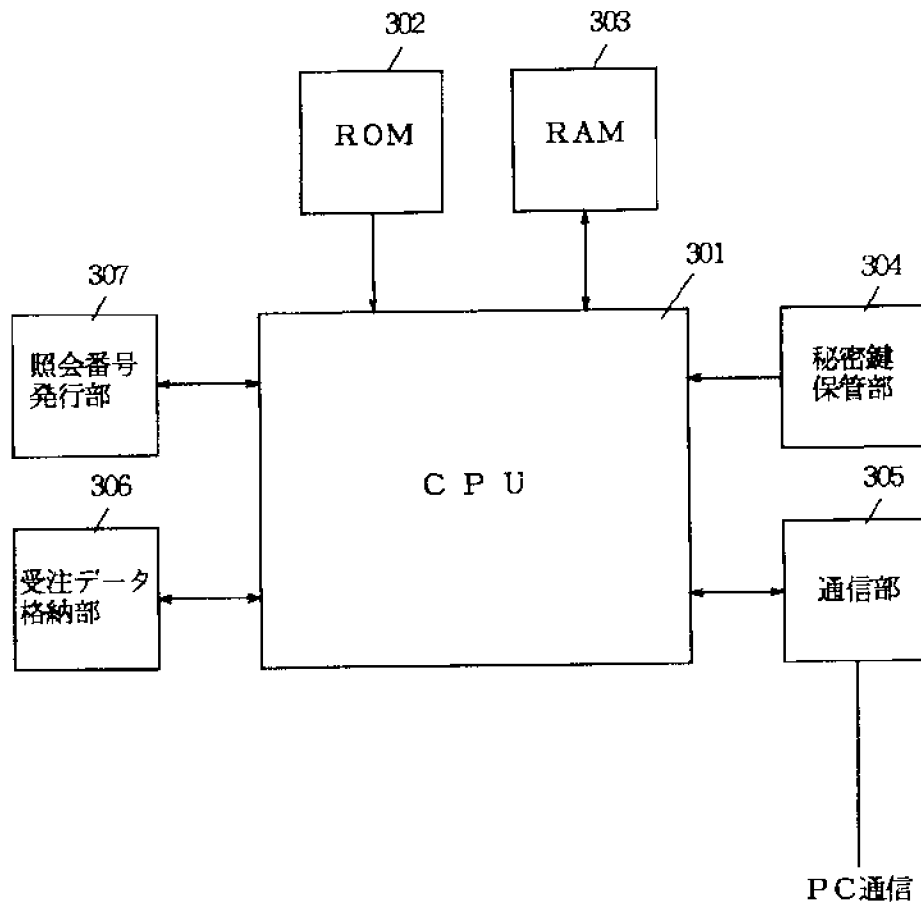
【図 1 4】

	受付部門 a	中継部門 b	商品部門 c
Idi	○	×	×
PID	×	×	○
Pr	○	○	○
Ref1	○	○	×
Ref2	×	○	○
rb	×	○	×
rc	×	×	○
EOrd1	○	○	×
EOrd2	×	○	○
RPDT1	×	○	○
RPDT2	○	○	×

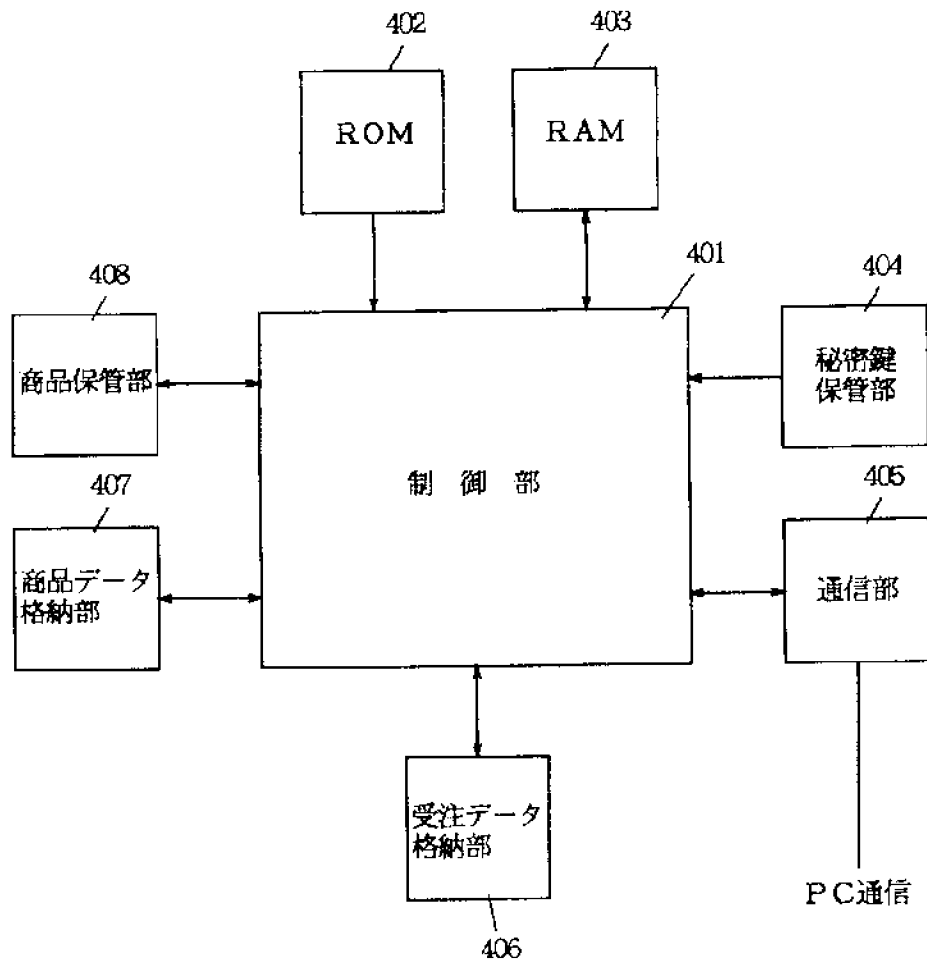
【図 3】



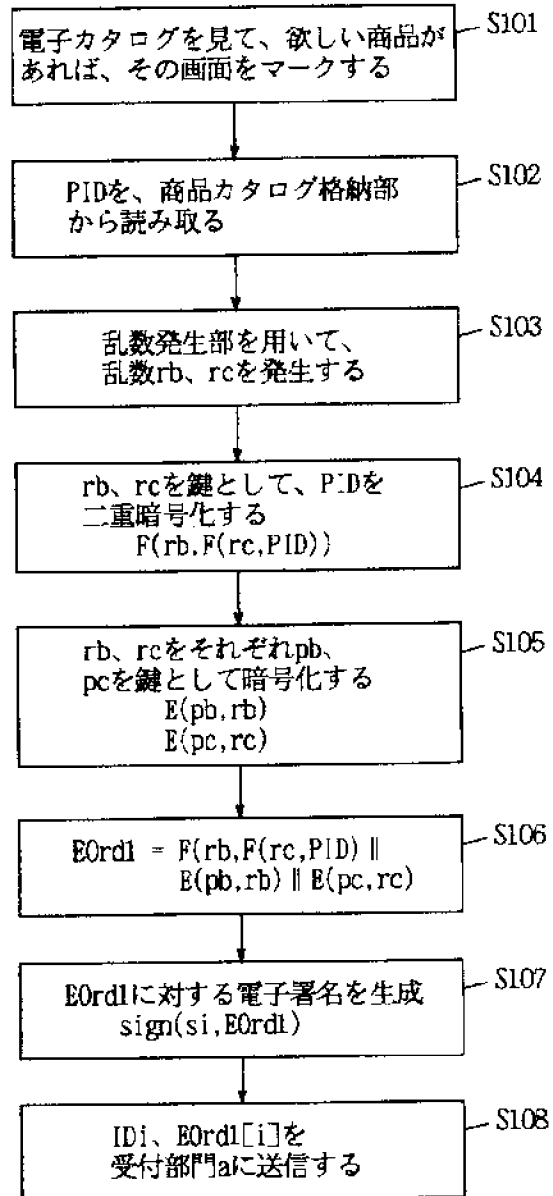
【図 4】



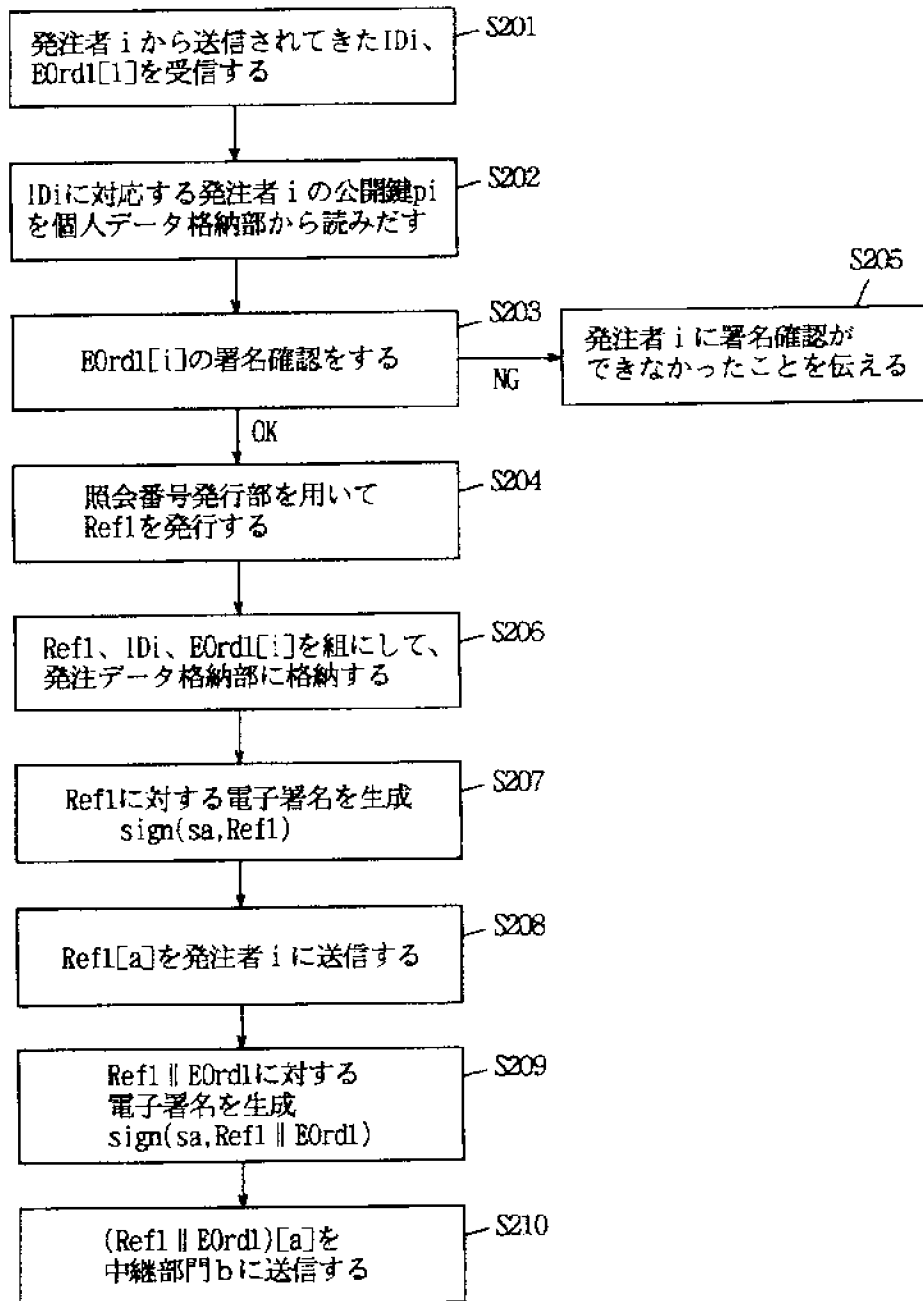
【図 5】



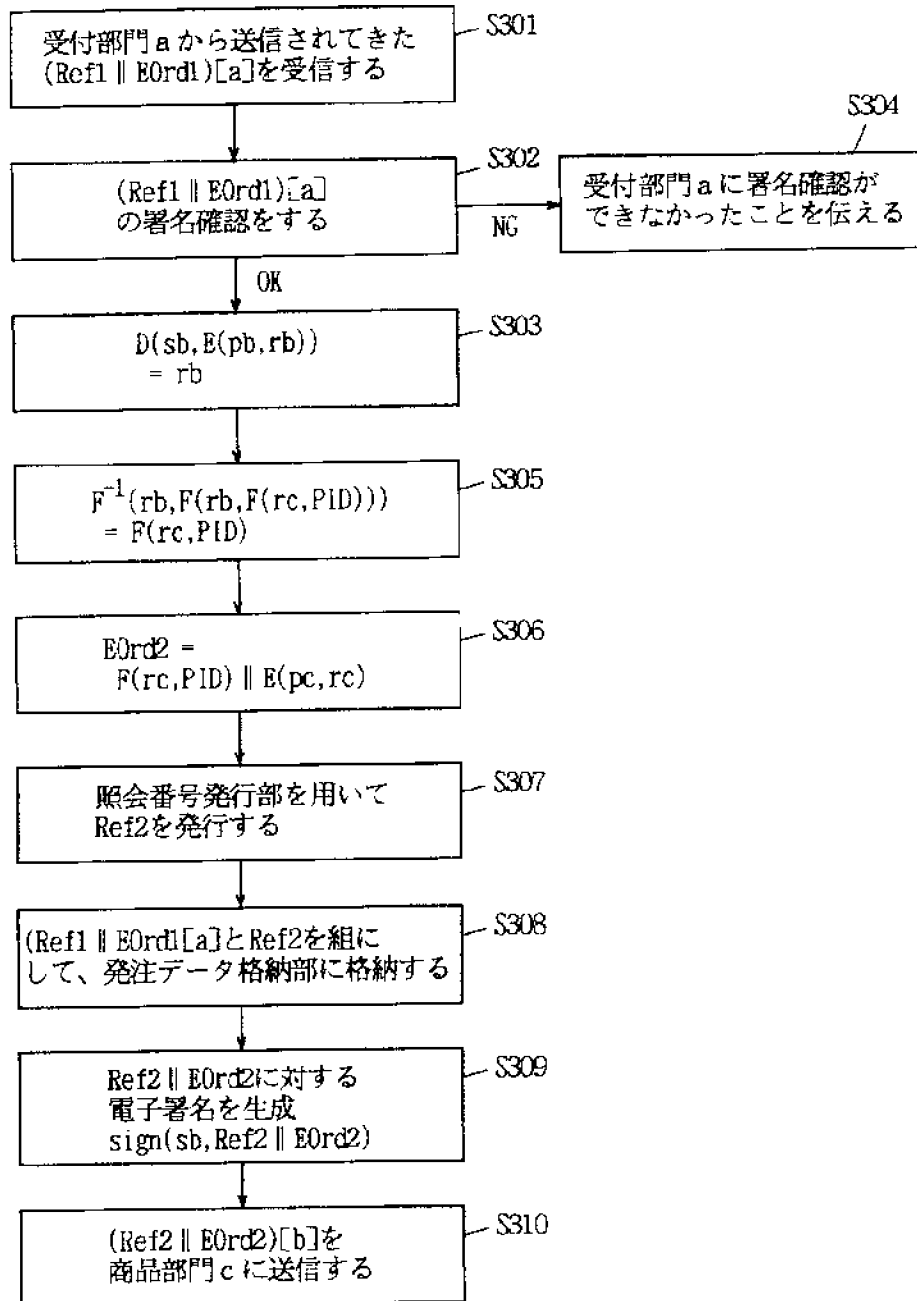
【図 7】



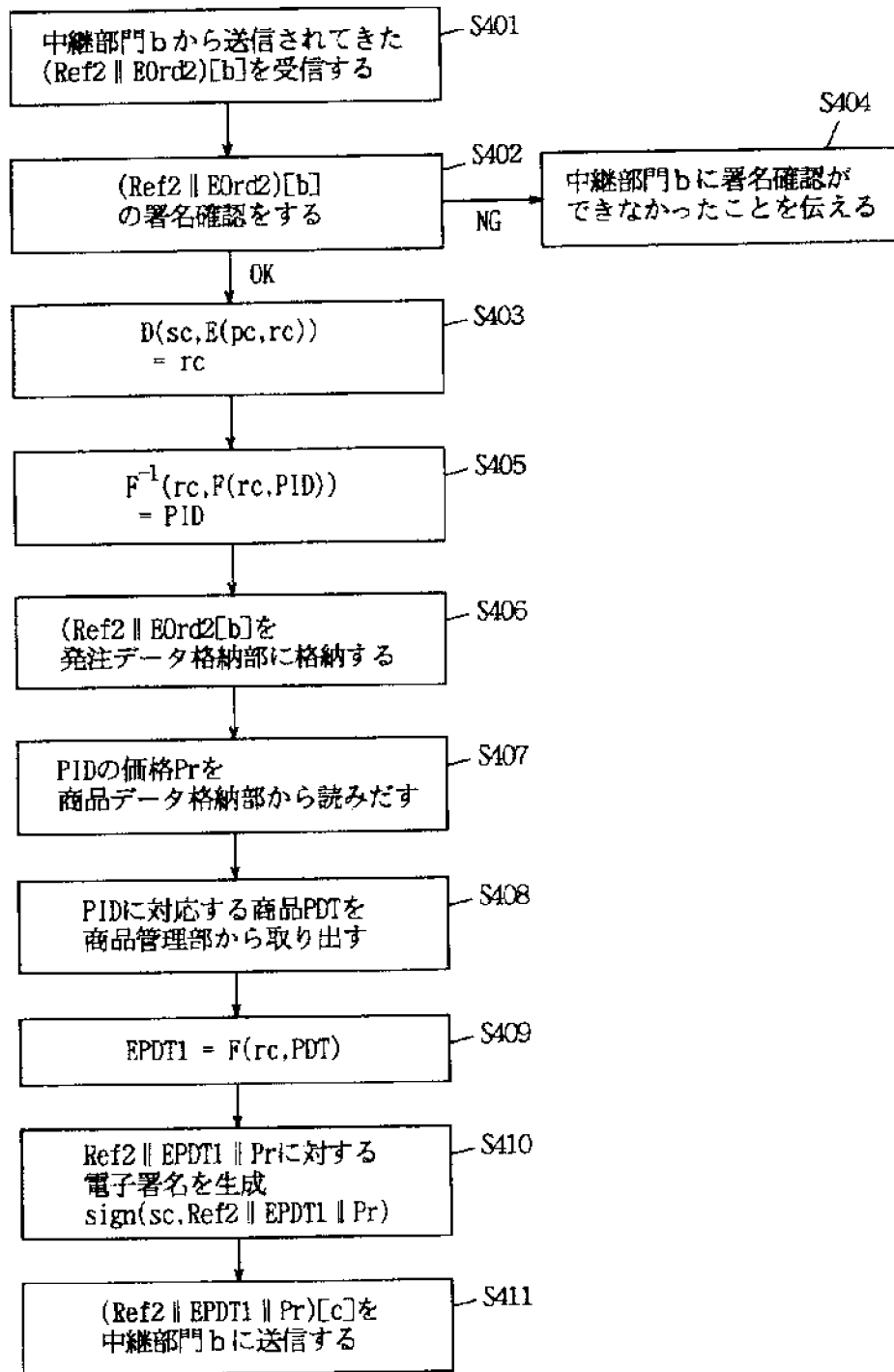
【図 8】



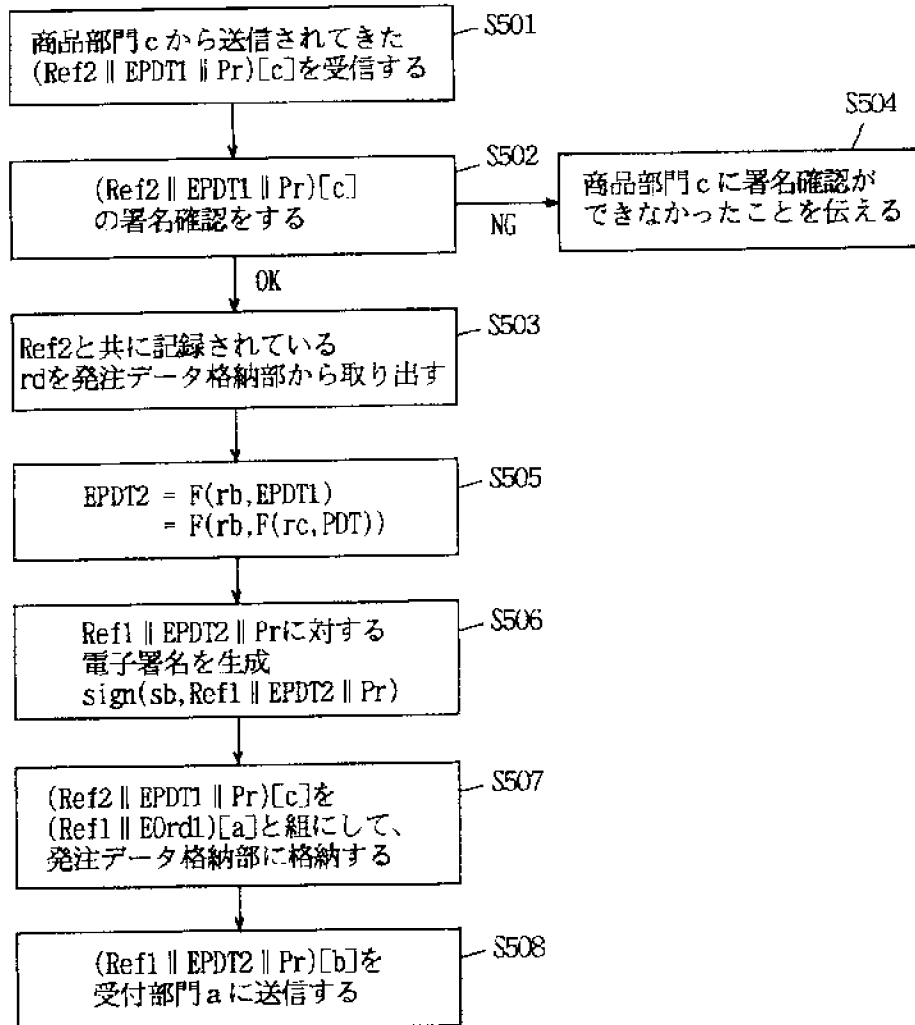
【図 9】



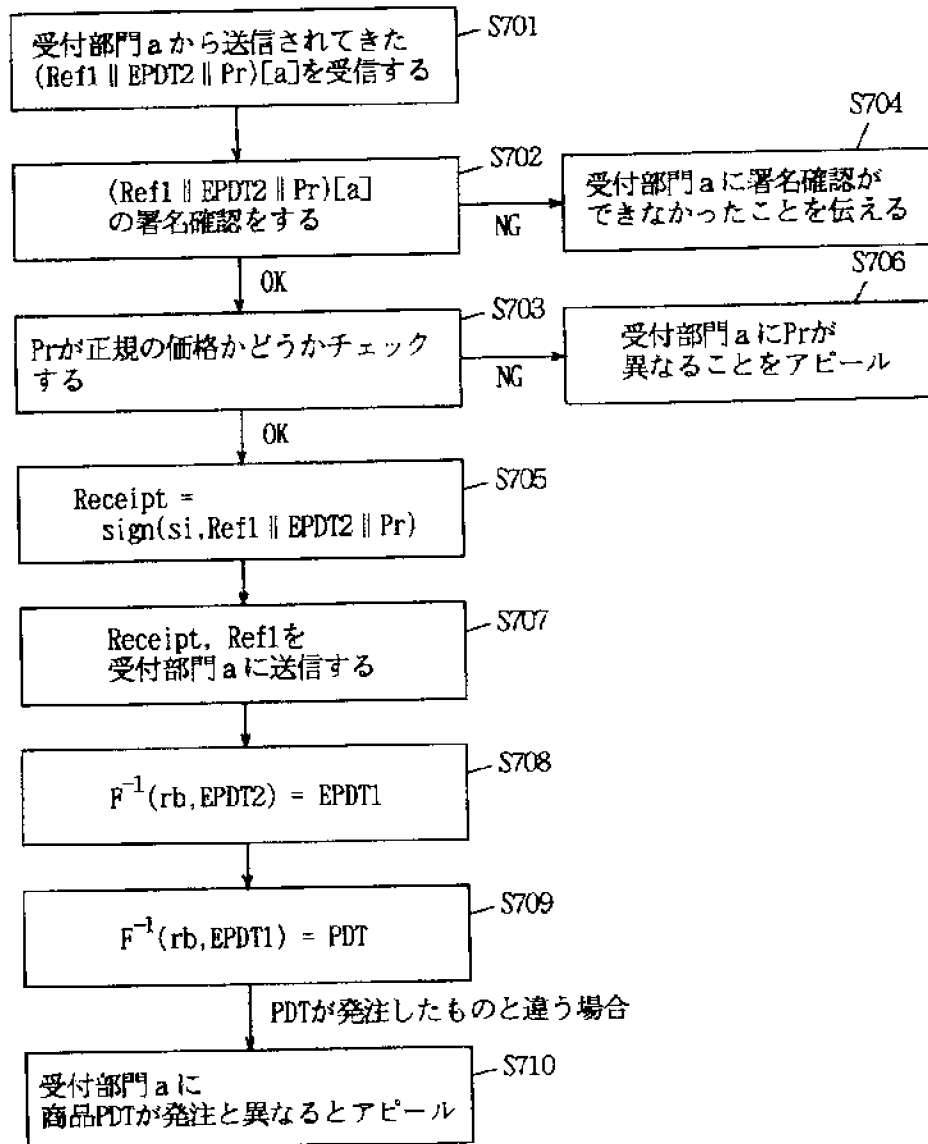
【図 10】



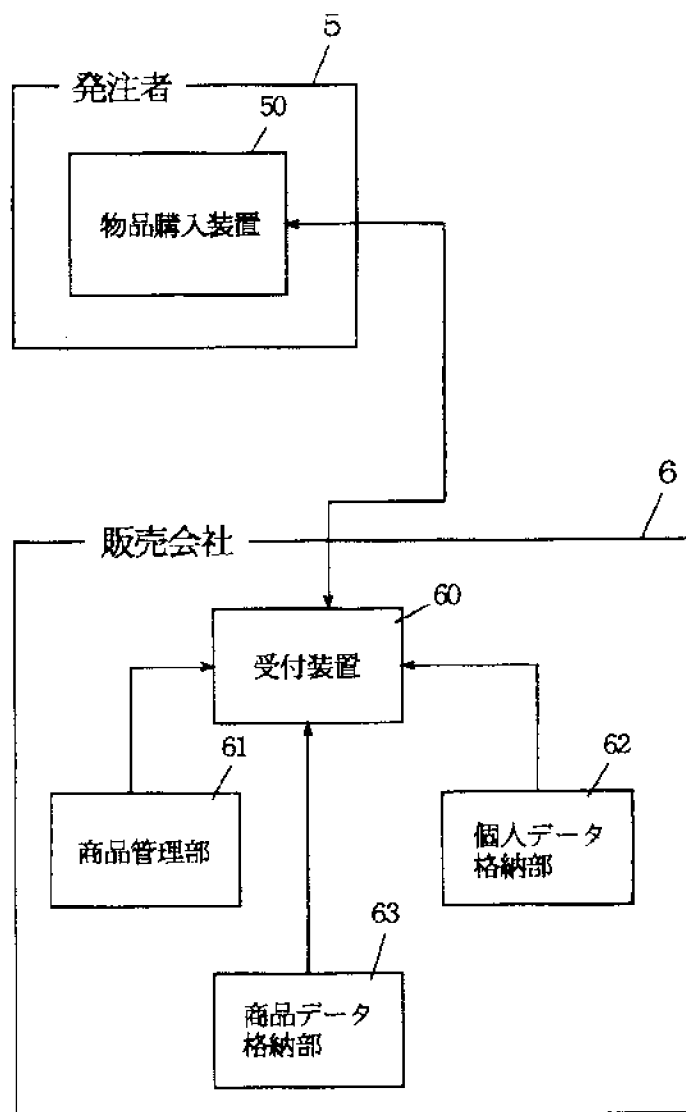
【図 1 1】



【図 1 3】



【図 15】



フロントページの続き

(51) Int. Cl.⁶

G 0 6 F 17/60

G 0 9 C 1/00

識別記号

庁内整理番号

F I

技術表示箇所

7259-5 J